(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 035 518 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
13.09.2000 Patentblatt 2000/37

(51) Int. Cl.⁷: **G07B 17/04**

(21) Anmeldenummer: **00250065.0**

(22) Anmeldetag: **25.02.2000**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **12.03.1999 DE 19912781**
15.06.1999 DE 19928057

(71) Anmelder: **Francotyp-Postalia Aktiengesellschaft & Co.**
16547 Birkenwerder (DE)

(72) Erfinder:
, Post, Peter
12357 Berlin (DE)
, Roseneau, Dirk
13469 Berlin (DE)
, Schlaaff, Torsten
16341 Zepernick (DE)

(54) Verfahren zum Schutz eines Sicherheitsmoduls und Anordnung zur Durchführung des Verfahrens

(57) Die Erfindung betrifft ein Verfahren zum Schutz eines Sicherheitsmoduls mit Zustandüberwachung, Überwachung des sachgemäßen Gebrauchs oder Austausches des Sicherheitsmoduls mittels einer ersten (120), zweiten (12) und dritten Funktionseinheit (13), Signalisieren mindestens eines Zustandes (220, 230, 240, 250, 260, 270, 280, 290) gesteuert mittels der ersten Funktionseinheit (120) und Löschen von sensitiven Daten aufgrund eines unsachgemäßen Gebrauchs oder Austausches mindestens mittels der zweiten Funktionseinheit (12). Weiterhin ist ein Sperren der Funktionalität mittels der dritten Funktionseinheit (13) aufgrund eines Austausches des Sicherheitsmoduls, Reinitialisieren der zuvor gelöschten sensitiven Daten nach sachgemäßem Gebrauch oder Austausch des Sicherheitsmoduls (100) und Wiederinbetriebnahme durch Freischalten der Funktionseinheiten des Sicherheitsmodules.
Die Anordnung zur Durchführung des Verfahrens, weist Mittel zum Laden mindestens eines von der Datenzentrale vorgegebenen Zeitkredits und eine mit einem Signalmittel (107, 108) verbundene erste Funktionseinheit (120) auf, wobei das Laden bei der Installation und beim Nachladen in einen Speicher (124) des Sicherheitsgerätes vorgenommen wird, und wobei die erste Funktionseinheit (120) einen Tageskredit auf Zeitablauf auswertet und das Signalmittel (107, 108) ansteuert, mindestens um den Zeitablauf zusignalisieren. Der Sicherheitsmodul kann verschiedene Zustände signalisieren. So kann beispielsweise unterschieden werden, ob der letzte Kontakt zur Datenzentrale sehr lange zurückliegt.

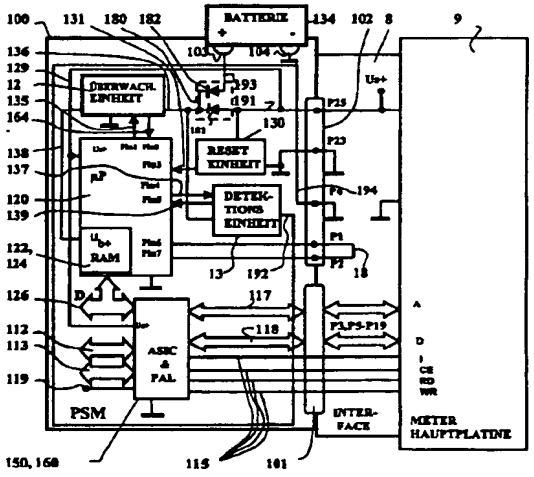


Fig. 1

EP 1 035 518 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Schutz eines Sicherheitsmoduls, gemäß der im Oberbegriff des Anspruchs 1 angegebenen Art, und eine Anordnung zur Durchführung des Verfahrens, gemäß der im Oberbegriff des Anspruchs 10 angegebenen Art. Ein solcher postalischer Sicherheitsmodul ist insbesondere für den Einsatz in einer Frankiermaschine bzw. Postbearbeitungsmaschine oder Computer mit Postbearbeitungsfunktion geeignet.

[0002] Moderne Frankiermaschinen, wie die aus der US 4.746.234 bekannte Thermotransfer-Frankiermaschine, setzen eine vollelektronische digitale Druckvorrichtung ein. Damit ist es prinzipiell möglich, beliebige Texte und Sonderzeichen im Frankierstempeldruckbereich und ein beliebiges oder ein einer Kostenstelle zugeordnetes Werbeklischee zu drucken. So hat zum Beispiel die Frankiermaschine T1000 der Anmelderin einen Mikroprozessor, welcher von einem gesicherten Gehäuse umgeben ist, das eine Öffnung für die Zuführung eines Briefes aufweist. Bei einer Briefzuführung übermittelt ein mechanischer Briefsensor (Mikroschalter) ein Druckanforderungssignal an den Mikroprozessor. Der Frankierabdruck beinhaltet eine zuvor eingegebene und gespeicherte postalische Information zur Beförderung des Briefes. Die Steuereinheit der Frankiermaschine nimmt eine Abrechnung softwaremäßig vor, übt eine Überwachungsfunktion ggf. bezüglich der Bedingungen für eine Datenaktualisierung aus und steuert das Nachladen eines Portwertguthabens.

[0003] Für die oben genannte Thermotransfer-Frankiermaschine wurde bereits in US 5,606,508 (DE 42 13 278 B1) und in US 5,490,077 eine Dateneingabemöglichkeit mittels Chipkarten vorgeschlagen. Eine der Chipkarten lädt neue Daten in die Frankiermaschine und ein Satz an weiteren Chipkarten gestattet durch das Stecken einer Chipkarte eine Einstellung entsprechend eingespeicherter Daten vorzunehmen. Das Datenladen und die Einstellung der Frankiermaschine kann damit bequemer und schneller als per Tastatureingabe erfolgen. Eine Frankiermaschine zum Frankieren von Postgut, ist mit einem Drucker zum Drucken des Postwertstempels auf das Postgut, mit einer Steuerung zum Steuern des Druckens und der peripheren Komponenten der Frankiermaschine, mit einer Abrecheneinheit zum Abrechnen von Postgebühren, mit mindestens einem nichtflüchtigen Speicher zum Speichern von Postgebührendaten, mit mindestens einem nichtflüchtigen Speicher zum Speichern von sicherheitsrelevanten Daten und mit einer Kalender/Uhr ausgestattet. Der nichtflüchtige Speicher der sicherheitsrelevanten Daten und/oder die Kalender/Uhr wird gewöhnlich von einer Batterie gespeist. Bei bekannten Frankiermaschinen werden sicherheitsrelevante Daten (kryptografische Schlüssel u.ä.) in nichtflüchtigen Speichern gesichert. Diese Speicher sind EEPROM, FRAM oder batteriegesicherte SRAM. Bekannte Frankiermaschinen verfügen oft auch über eine interne Echtzeituhr (Real Time Clock) RTC, die von einer Batterie gespeist wird. Bekannt sind z.B. vergossene Module, die integrierte Schaltkreise und eine Lithium-Batterie enthalten. Diese Module müssen nach Ablauf der Lebensdauer der Batterie im Ganzen ausgetauscht und entsorgt werden. Aus wirtschaftlichen und ökologischen Gesichtspunkten ist es günstiger, wenn nur die Batterie ausgetauscht werden muß. Dazu muß jedoch das Sicherheitsgehäuse geöffnet und anschließend wieder verschlossen und gesiegelt werden, denn die Sicherheit gegenüber Betrugsversuchen beruht im Wesentlichen auf dem gesicherten Gehäuse, welches die gesamte Maschine umschließt. Seitens der Anmelderin wurde in EP 660 269 A2 (US 5,671,146) bereits ein geeignetes Verfahren zur Verbesserung der Sicherheit von Frankiermaschinen vorgeschlagen, in welchem zwischen einem authorisierten und unauthorisierten Öffnen des Sicherheitsgehäuses unterschieden wird.

[0004] Eine eventuell erforderliche Reparatur einer Frankiermaschine ist dann vor Ort nur schwer möglich, wenn der Zugang zu den Bauteilen erschwert oder eingeschränkt ist. Bei größeren Postverarbeitungsmaschinen oder sogenannten PC-Frankierern wird zukünftig das gesicherte Gehäuse auf das sogenannte postalische Sicherheitsmodul reduziert werden, was die Zugänglichkeit zu den übrigen Bauteilen verbessern kann.Zum wirtschaftlichen Austauschen der Batterie des Sicherheitsmoduls wäre es außerdem wünschenswert, daß sich diese auf relativ einfachem Wege auswechseln läßt. Dazu muß sich die Batterie außerhalb des Sicherheitsbereichs der Frankiermaschine befinden. Wenn die Batterieklemmen aber von außen zugänglich gemacht werden, ist ein möglicher Angreifer in der Lage, die Batteriespannung zu manipulieren. Bekannte batteriegespeiste SRAM und RTC haben bzgl. ihrer geforderten Betriebsspannung unterschiedliche Anforderungen. Die notwendige Spannung zum Halten von Daten von SRAM liegt unterhalb der geforderten Spannung zum Betrieb von RTC. Daß bedeutet, daß ein Verringern der Spannung unter einen bestimmten Grenzwert zu einem unerwünschten Verhalten der Komponenten führt: Die RTC bleibt stehen, die Uhrzeit - gespeichert in SRAM-Zellen - und die Speicherinhalte des SRAM bleiben erhalten. Wenigstens eine der Sicherheitsmaßnahmen, beispielsweise Long Time Watchdogs, wären dann auf der Frankiermaschinenseite unwirksam. Unter Long Time Watchdogs wird folgendes verstanden: Die enifernte Datenzentrale gibt einen Zeitkredit bzw. eine Zeitdauer, insbesondere eine Anzahl von Tagen, oder einen bestimmten Tag vor, bis zu welchem sich die Frankiereinrichtung per Kommunikationsverbindung melden kann. Nach erfolglosen Ablauf des Zeitkredits oder der Frist wird das Frankieren verhindert. Unter dem Titel: Verfahren und Anordnung zur Erzeugung und Überprüfung eines Sicherheitsabdruckes wurde bereits in der EP 660 270 A2 (US 5,680,463) ein Verfahren vorgeschlagen, die voraussichtliche Zeitdauer bis zur nächsten Guthabennachladung zu ermitteln, wobei seitens einer Datenzentrale diejenige Frankiermaschine als suspekt gilt, welche sich nicht fristgemäß meldet. Suspekte Frankiermaschinen werden der Postbehörde mitgeteilt, welche den Poststrom nach von suspekten Frankiermaschinen frankierten Briefen überwacht. Ein Ablauf des Zeitkredits oder der Frist wird bereits auch von der Frankiereinrichtung ermittelt. Der Benutzer wird aufgefordert die überfällige Kommunikation durchzuführen. Diese Frankiereinrichtung besitzt jedoch kein separates Sicherheitsmodul.

[0005] Sicherheitsmodule sind von elektronischen Datenverarbeitungsanlagen her bereits bekannt. Zum Schutz vor Einbruch in eine elektronische Anlage wird in EP 417 447 B1 bereits eine Sperre vorgeschlagen, welche Stromversorgungsmittel- und Signalerfassungsmittel sowie Abschirmmittel im Gehäuse umfaßt. Das Abschirmmittel besteht aus Einkapselungsmaterial und Leitungsmitteln, an welchen die Stromversorgungs- und Signalerfassungsmittel angeschlossen sind. Letzteres reagiert auf eine Veränderung des Leitungswiderstandes des Leitungsmittels. Außerdem

enthält das Sicherheitsmodul eine interne Batterie, einen Spannungsumschalter von Systemspannung auf Batteriespannung, ein Power Gate und einen Kurzschlußtransistor sowie weitere Sensoren. Wenn die Spannung eine bestimmte Grenze unterschreitet, reagiert das Power Gate. Wenn der Leitungswiderstand, die Temperatur oder die Strahlung verändert ist, reagiert die Logik. Mittels des Power Gate oder mittels der Logik wird der Ausgang des Kurzschlußtransistor auf L-Pegel umgeschaltet, wodurch ein im Speicher gespeicherter kryptographischer Schlüssel gelöscht wird. Jedoch ist die Lebensdauer der nicht auswechselbaren Batterie und damit des Sicherheitsmoduls für den Einsatz in Frankiereinrichtungen bzw. Postverarbeitungsmaschinen zu klein.

[0006] Eine größere Postverarbeitungsmaschine ist beispielsweise die JetMail®. Ein Frankierdruck wird hier mittels einem stationär angeordneten Tintenstrahldruckkopf bei einem nichtwaagerechten annähernd vertikalen Brieftransport erzeugt. Eine geeignete Ausführung für eine Druckvorrichtung wurde bereits in der DE 196 05 015 C1 vorgeschlagen. Die Postverarbeitungsmaschine hat ein Meter und eine Base. Soll das Meter mit einem Gehäuse ausgestattet werden, so daß Bauteile leichter zugänglich sind, dann muß es durch ein postalisches Sicherheitsmodul vor Betrugsversuchen geschützt werden, welches mindestens das Abrechnen der Postgebühren durchführt. Um Einflüsse auf den Programmverlauf auszuschließen, wurde bereits in der EP 789 333 A2 unter dem Titel: Frankiermaschine vorgeschlagen, ein Sicherheitsmodul mit einer Anwenderschaltung (Application Specific Integrated Circuit) ASIC auszustatten, die eine Hardware-Abrecheneinheit aufweist. Die Anwenderschaltung steuert außerdem die Druckdatenübertragung zum Druckkopf.

[0007] Letzteres wäre nur dann nicht erforderlich, wenn für jedes Poststück einzigartige Abdruke erzeugt werden. Ein geeignetes Verfahren und Anordnung zur Erzeugung und Überprüfung eines Sicherheitsabdruckes ist beispielsweise in den US 5,680,463, US 5,712,916 und US 5,734,723 vorgeschlagen worden. Dabei wird eine spezielle Sicherheitsmarkierung elektronisch generiert und in das Druckbild eingebettet.

[0008] Weitere Maßnahmen zum Schutz eines Sicherheitsmodul vor einem Angriff auf die in ihm gespeicherten Daten wurden auch in den nicht vorveröffentlichten deutschen Anmeldungen 198 16 572.2 und 198 16 571.4 vorgeschlagen. Bei einer Vielzahl von Sensoren steigt der Stromverbrauch und ein nicht ständig von einer Systemspannung versorgter Sicherheitsmodul zieht dann den für die Sensoren benötigten Strom aus seiner internen Batterie, was letztere ebenfalls frühzeitig erschöpft. Die Kapazität der Batterie und der Stromverbrauch beschränken somit die Lebensdauer eines Sicherheitsmoduls.

[0009] Frankiermaschinen sind wie viele andere Produkte ebenfalls modular aufgebaut. Diese Modularität ermöglicht den Austausch von Modulen und Komponenten aus verschiedenen Gründen. So können z.B. defekte Module ausgetauscht und durch überprüfte, reparierte oder neue Module ersetzt werden. Da eine höchste Sorgsamkeit beim Austausch von Baugruppen erforderlich ist, die sicherheitsrelevante Daten enthalten, erfordert der Austausch in der Regel den Einsatz eines Service Technikers und Maßnahmen, die bei unsachgemäßem Gebrauch bzw. unauthorisierten Austausch eines Sicherheitsmoduls dessen Funktionsweise unterbinden. Letzteres ist aber sehr aufwendig.

[0010] Der Erfindung liegt die Aufgabe zugrunde, mit geringem Aufwand den Schutz vor einem unbefugt manipulierten Sicherheitsmodul zu gewährleisten, wenn das Sicherheitsmodul austauschbar angeordnet ist. Der Austausch soll von jederman auf möglichst einfache Weise möglich sein.

[0011] Die Aufgabe wird mit den Merkmalen des Verfahrens nach Anspruch 1 und mit den Merkmalen der Anordnung nach Anspruch 10 gelöst.

[0012] Die Erfindung geht davon aus, mittels Funktionseinheiten den Austausch, die Manipulation und den Gebrauch eines Sicherheitsmoduls einer Frankiermaschine, Postverarbeitungseinrichtung oder ähnlichen Gerätes festzustellen, um den Benutzern der verschiedenen Geräte eine Gewährleistung über die korrekte Funktionsweise des Sicherheitsmoduls und damit des gesamten Gerätes bieten zu können. Ein Austauschen oder Beschädigen des Sicherheitsmoduls wird mindestens detektiert und ggf. nachträglich als Zustand signalisiert, wenn der Sicherheitsmodul wieder gesteckt ist und mit einer Systemspannung versorgt wird. Die Veränderungen des Zustandes des Sicherheitsmoduls werden mittels einer ersten Funktionseinheit und mittels einer Detektionseinheit erfaßt, welche eine rücksetzbare Selbsthaltung aufweist und von einer Batterie versorgt wird. Die erste Funktionseinheit kann den jeweiligen Zustand auswerten, wenn sie wieder mit Systemspannung versorgt wird. Die Vorteile liegen in einer schnellen Reaktion auf Veränderungen des Zustandes des Sicherheitsmoduls und in einem geringem Batteriestromverbrauch der Detektionseinheit auch während der Nichtversorgung mit der Systemspannung.

[0013] Eine zweite Funktionseinheit kann die Batteriespannung gegebenenfalls daraufhin überwachen, ob deren Kapazität erschöpft ist. Ein erforderlicher Batteriewechsel wird signalisiert, wobei natürlich eine Versorgung durch die Systemspannung gesichert sein muß. Es ist mindestens dann von einem unsachgemäßem Gebrauch eines Sicherheitsmoduls bei dem Austausch auszugehen, bei welchen nicht nur die Systemspannung fehlt, sondern auch die austauschbar angeordnete Batterie entfernt wird. Damit der Austausch von möglichst gering qualifiziertem Personal und in Zukunft gar durch den Benutzer ausgeführt werden kann, übernimmt die zweite Funktionseinheit die Überwachung auf Spannungsausfall beim Austausch der Batterie, wobei die erste Funktionseinheit erforderlichenfalls zunächst sensitive Daten löscht und damit den weiteren Gebrauch des Sicherheitsmoduls einschränkt oder gar unterbindet. Nach einer vor-Ort-Inspektion des Sicherheitsmoduls durch einen Service, kann bei intaktem Gehäuse, der ursprüngliche Funktionsumfang wiederhergestellt werden. Die erste Funktionseinheit erzwingt bei einer späteren Wiederinbetriebnahme eine Kontaktaufnahme des Sicherheitsmoduls mit einer entfernten Datenzentrale zum Freischalten mindestens einer Funktionseinheit. Falls ohne Batteriewechsel der ganze Sicherheitsmodul ausgetauscht wurde, werden zunächst durch die zweite Funktionseinheit ebenfalls sensitive Daten gelöscht, jedoch können bei der Wiederinbetriebnahme die sensitiven Daten reinitialisiert werden. Zur Kontaktaufnahme sind Verfahren mit einer digitalen oder analogen Übertragungsstrecke einsetzbar. Ebenfalls wird eine Inspektion des Sicherheitsmoduls dann

durch einen Service veranlaßt. Der Sicherheitsmoduls kann verschiedene Zustände signalisieren. So kann beispielsweise unterschieden werden, ob der letzte Kontakt zur Datenzentrale solange zurückliegt, daß dies bereits verdächtig erscheint oder zulange, daß eine Reinitialisierung nicht mehr gestattet wird. Die erste Funktionseinheit wertet ständig einen ersten Tageskredit aus. Wenn letzterer erschöft ist, wird der suspekte Zustand signalisiert. Durch Kontaktaufnahme mit der Datenzentrale kann der nor-male Arbeitszustand wiederhergestellt werden, ohne daß eine Inspektion vor Ort durch einen Service erforderlich wird. Der Zeitkredit kann variabel und von Sicherheitsgerät zu Sicherheitsgerät unterschiedlich sein. Der Zeitkredit kann von der Datenzentrale vorgegeben und bei der Installation in einen Speicher des Sicherheitsgerätes geladen werden. Die erste Funktionseinheit wertet ständig einen zweiten Tageskredit aus. Wenn letzterer erschöft ist, wird der Zustand „LOST" signalisiert. Im letzteren Fall wird ebenfalls eine Inspektion des Sicherheitsmoduls durch einen Service vor Ort erforderlich.

[0014] Das Verfahren zum Schutz eines Sicherheitsmoduls beinhaltet die folgenden Schritte:

- Überwachung des Zustandes, des sachgemäßen Gebrauchs oder Austausches des Sicherheitsmoduls mindestens mittels zweier Funktionseinheiten,
- Signalisieren mindestens eines Zustandes gesteuert mittels einer ersten Funktionseinheit,
- Löschen von sensitiven Daten aufgrund eines unsachgemäßen Gebrauchs oder Austausches mindestens mittels einer zweiten Funktionseinheit.

[0015] Dann erfolgt ein weiterer Verfahrensablauf mit den Schritten:

- Reinitialisieren mittels der ersten Funktionseinheit von zuvor gelöschten sensitiven Daten nach sachgemäßem Gebrauch oder Austausch des Sicherheitsmoduls,
- Wiederinbetriebnahme durch Freischalten der Funktionseinheiten des Sicherheitsmodules.

[0016] Gegebenenfalls muß ein Austausch des Sicherheitsmoduls vorgenommen werden. Mittels einer dritten Funktionseinheit kann sowohl ein Austausch- als auch ein Zerstörungszustand nach einem mechanischen oder chemischen Angriff detektiert werden, mit dem Schritt:

- Sperren der Funktionalität mittels der dritten Funktionseinheit aufgrund eines Austausches des Sicherheitsmoduls oder aufgrund eines Zerstörungszustandes nach einem Angriff.

[0017] Es ist vorgesehen, daß das Reinitialisieren in Verbindung mit einer Kommunikation mittels einer entfernten Datenzentrale von der ersten Funktionseinheit vorgenommen wird, nachdem eine dynamische Gestecktsein-Detektion erfolgreich durchgeführt wurde, wobei während der Detektion von der ersten Funktionseinheit über eine Stromschleife der Interfaceeinheit Informationen ausgetauscht werden, deren fehlerfreie Übermittlung den Beweis für den sachgemäßen Einbau des Sicherheitsmodules erbringt. Das Freischalten von Funktionseinheiten des Sicherheitsmodules erfolgt durch deren Rücksetzen. Die erste Funktionseinheit ist ein mit den anderen Funktionseinheiten verbundener Prozessor, welcher programmiert ist, den jeweiligen Zustand festzustellen. Die zweite Funktionseinheit ist eine Spannungsüberwachungseinheit mit rücksetzbarer Selbsthaltung und die dritte Funktionseinheit ist eine Detektionsschaltung mit rücksetzbarer Selbsthaltung, die einen vorhergegangenen Ungestecktsein-Zustand und ebenso einen Zerstörungszustand nach einem mechanischen oder chemischen Angriff detektieren kann. Für diese statische Detektion ist die Vergußmasse mit zusätzlichen Mitteln ausgestattet, welche das Sicherheitsmodul bei einem Angriff warnen und ggf. schützen.

[0018] Die Anordnung zur Durchführung des Verfahrens hat ein Sicherheitsmodul, mit einer Logik mit Mitteln zur Versorgung des Sicherheitsmoduls mit einer Systemspannung oder mit einer Spannung aus einer Batterie und mit einer Anzahl an Überwachungsmitteln. Sie ist gekennzeichnet durch mindestens eine erste und zweite Funktionseinheit sowie durch Mittel zum Laden mindestens eines von der Datenzentrale vorgegebenen Zeitkredits und durch ein Signalmittel, welches mit einer ersten Funktionseinheit verbunden ist, wobei das Laden bei der Installation und beim Nachladen in einen Speicher des Sicherheitsgerätes vorgenommen wird, und wobei die erste Funktionseinheit einen Tageskredit auf Zeitablauf auswertet und das Signalmittel ansteuert, mindestens um den Zeitablauf zu signalisieren, sowie durch Mittel der zweiten Funktionseinheit zum Löschen von sensitiven Daten im Speicher aufgrund eines unsachgemäßen Gebrauchs oder Austausches des Sicherheitsmoduls.

[0019] Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Figur 1, Blockbild und Interface des Sicherheitsmoduls,

Figur 2, Blockschaltbild der Frankiermaschine,

Figur 3, Perspektivische Ansicht der Frankiermaschine von hinten,

Figur 4, Blockschaltbild des Sicherheitsmoduls (zweite Variante),

Figur 5, Schaltbild der Detektionseinheit,

Figur 6, Seitenansicht des Sicherheitsmoduls (1 .Variante),

Figur 7, Draufsicht auf das Sicherheitsmodul (1 .Variante),

Figur 8a, Ansicht des Sicherheitsmoduls von rechts (1 .Variante),

Figur 8b, Ansicht des Sicherheitsmoduls von links (1 .Variante),

Figur 9, Tabelle für Statussignalisierung,

Figur 10, Darstellung der Prüfungen im System für statische und dynamisch änderbare Zustände,

Figur 11, Seitenansicht des Sicherheitsmoduls (2.Variante),

Figur 12, Draufsicht auf das Sicherheitsmodul (2.Variante),

Figur 13a, Ansicht des Sicherheitsmoduls von rechts (2.Variante),

Figur 13b, Ansicht des Sicherheitsmoduls von links (2.Variante).

[0020] In der Figur 1 ist ein Blockbild des Sicherheitsmoduls 100 mit den Kontaktgruppen 101, 102 zum Anschluß an ein Interface 8 sowie mit den Batteriekontaktklemmen 103 und 104 eines Batterieinterfaces für eine Batterie 134 dargestellt. Obwohl das Sicherheitsmodul 100 mit einer harten Vergußmasse vergossen ist, ist die Batterie 134 des Sicherheitsmoduls 100 außerhalb der Vergußmasse auf einer Leiterplatte auswechselbar angeordnet. Die Leiterplatte trägt die Batteriekontaktklemmen 103 und 104 für den Anschluß der Pole der Batterie 134. Mittels der Kontaktgruppen 101, 102 wird das Sicherheitsmodul 100 an ein entsprechendes Interface 8 der Hauptplatine (Motherboard) 9 gesteckt. Die erste Kontaktgruppe 101 steht mit dem Systembus einer Steuereinrichtung in Kommunikationsverbindung und die zweite Kontaktgruppe 102 dient der Versorgung des Sicherheitsmoduls 100 mit der Systemspannung. Über die Pins P3,P5-P19 der Kontaktgruppe 101 laufen Adreßund Datenleitungen 117, 118 sowie Steuerleitungen 115. Die erste und/oder zweite Kontaktgruppe 101 und/oder 102 sind/ist zur statischen und dynamischen Überwachung des Angestecktseins des Sicherheitsmoduls 100 ausgebildet. Über die Pins P23 und P25 der Kontaktgruppe 102 wird die Versorgung des Sicherheitsmodul 100 mit der Systemspannung der Hauptplatine 9 realisiert und über die Pins P1, P2 bzw. P4 wird eine dynamische und statische Ungestecktsein-Detektion durch das Sicherheitsmodul 100 realisiert. Letztere erfordert eine Detektionseinheit 13, welche über über eine Leiterschleife 192, 194 mit dem Pin P4 der Kontaktgruppe 102 verbunden ist. Die Leiterschleife kann als Bestandteil des besonders zu sichernden Teils des Sicherheitsmoduls 100 ausgebildet und in Vergußmasse so eingebettet sein, das bei einem mechanisch oder chemischen Angriff auf den vorgenannten Teil des Sicherheitsmoduls 100 der Kontakt zum Pin P4 unterbrochen wird.
Das Sicherheitsmodul 100 weist in an sich bekannter Weise einen Mikroprozessor 120 auf, der einen - nicht gezeigten - integrierten Festwertspeicher (internal ROM) mit dem speziellen Anwendungsprogramm enthält, was für die Frankiermaschine von der Postbehörde bzw. vom jeweiligen Postbeförderer zugelassen ist. Alternativ kann an den internen Datenbus 126 ein üblicher Festwertspeicher ROM oder FLASHSpeicher angeschlossen werden.
Das Sicherheitsmodul 100 weist in an sich bekannter Weise eine ResetSchaltungseinheit 130, einen Anwenderschaltkreis ASIC 150 und eine Logik PAL 160 auf, die für den ASIC als Steuersignalgenerator dient. Die Reset-Schaltungseinheit 130 bzw. der Anwenderschaltkreis ASIC 150 und die Logik PAL 160 sowie eventuell weitere - nicht gezeigte - Speicher werden über die Leitungen 191 bzw. 129 mit Systemspannung Us+ versorgt, welche bei eingeschalteter Frankiereinrichtung von der Hauptplatine 9 geliefert wird. In der EP 789 333 A2 wurden bereits die wesentlichen Teile eines postalischen Sicherheitsmoduls PSM erläutert, die die Funktionen Abrechnen und Absichern der Postgebührendaten realisieren.

[0021] Die Systemspannung Us+ liegt außerdem über eine Diode 181 und die Leitung 136 am Eingang der Spannungsüberwachungseinheit 12 an. Am Ausgang der Spannungsüberwachungseinheit 12 wird eine zweite Betriebsspannung Ub+ geliefert, welche über die Leitung 138 zur Verfügung steht. Bei ausgeschalteter Frankiereinrichtung steht nicht die Systemspannung Us+, sondern nur die Batteriespannung Ub+ zur Verfügung. Die am negativen Pol liegende Batteriekontaktklemme 104 ist mit Masse verbunden. Von der am positiven Pol liegenden Batteriekontaktklemme 103 wird Batteriespannung über eine Leitung 193, über eine zweite Diode 182 und die Leitung 136 an den Eingang der Spannungsüberwachungseinheit geliefert. Alternativ zu den beiden Dioden 181, 182 kann ein handelsüblicher Schaltkreis als Spannungsumschalter 180 eingesetzt werden.

[0022] Der Ausgang der Spannungsüberwachungseinheit 12 ist über eine Leitung 138 mit einem Eingang für diese zweite Betriebsspannung U_{b+} des Prozessors 120 verbunden, welcher mindestens auf einen RAMSpeicherbereich 122,

124 führt und dort eine nichtflüchtige Speicherung solange garantiert, wie die zweite Betriebsspannung U_{b+} in der erforderlichen Höhe anliegt. Der Prozessor 120 enthält vorzugsweise einen internen RAM 124 und eine Echtzeituhr (RTC) 122.

[0023] Die Spannungsüberwachungseinheit 12 im Sicherheitsmodul weist eine rücksetzbare Selbsthaltung auf, die vom Prozessor 120 über eine Leitung 164 abgefragt und über eine Leitung 135 zurückgesetzt werden kann. Für eine Rücksetzung der Selbsthaltung weist die Spannungsüberwachungseinheit 12 Schaltungsmittel auf. Die Rücksetzung ist erst auslösbar, wenn die Batteriespannung über die vorbestimmte Schwelle angestiegen ist. Die Leitungen 135 and 164 sind je mit einem Pin (Pin1 und 2) des Prozessors 120 verbunden. Die Leitung 164 liefert ein Statussignal an den Prozessor 120 und die Leitung 135 liefert ein Steuersignal an die Spannungsüberwachungseinheit 12.

[0024] Die Leitung 136 am Eingang der Spannungsüberwachungseinheit 12 versorgt zugleich eine Ungestecktsein-Detektionseinheit 13 mit Betriebsoder Batteriespannung. Die Ungestecktsein-Detektionseinheit 13 gibt auf der Leitung 139 ein Statussignal an einen Pin 5 des Prozessors 120 ab, das eine Aussage über den Zustand der Schaltung gibt. Vom Prozessor 120 wird der Zustand der Ungestecktsein-Detektionseinheit 13 über die Leitung 139 abgefragt. Der Prozessor kann mit einem vom Pin 4 des Prozessors 120 über die Leitung 137 abgegebenen Signal die Ungestecktsein-Detektionseinheit 13 zurücksetzen. Nach dem Setzen wird eine statische Prüfung auf Anschluß durchgeführt. Dazu wird über eine Leitung 192 Massepotential abgefragt, welches am Anschluß P4 des interfaces 8 des postalischen Sicherheitsmoduls PSM 100 anliegt und nur abfragbar ist, wenn der Sicherheitsmodul 100 ordnungsgemäß gesteckt ist. Bei gesteckten Sicherheitsmodul 100 wird Massepotential des negativen Pols 104 der Batterie 134 des postalischen Sicherheitsmoduls PSM 100 auf den Anschluß P23 des Interfaces 8 gelegt und ist somit am Anschluß P4 des Interfaces 8 über die Leitung 192 von der Ungestecktsein-Detektionseinheit 13 abfragbar.

[0025] An den Pins 6 und 7 des Prozessors 120 liegt eine Leitungsschleife, welche über die Pins P1 und P2 der Kontaktgruppe 102 des Interfaces 8 zum Prozessor 120 zurückgeschleift wird. Zur dynamischen Prüfung des Angeschlossenseins des postalischen Sicherheitsmoduls PSM 100 an der Hauptplatine 9 werden vom Prozessor 120 wechselnde Signalpegel in ganz unregelmäßigen Zeitabständen an die Pin's 6, 7 angelegt und über die Schleife zurückgeschleift.

Das postalische Sicherheitsmodul PSM 100 ist mit einer Long-LiveBatterie bestückt, welches auch eine Überwachung des Gebrauchs ermöglicht, ohne das das Sicherheitsmodul an einer Systemspannung eines Postverabeitungseinrichtung liegt. Der sachgemäße Gebrauch, Betrieb, Installation oder Einbau in der geeigneten Umgebung sind solche von den Funktionseinheiten des Sicherheitsmoduls zu prüfende Eigenschaften. Eine Erstinstallation wird vom Hersteller des postalischen Sicherheitsmoduls vorgenommen. Es ist also nach dieser Erstinstallation zunächst lediglich zu prüfen, ob das postalische Sicherheitsmodul von ihrem Einsatzfeld (Postverabeitungseinrichtung) getrennt wird, wobei dies in der Regel bei einem Austausch erfolgt.

Die Überwachung dieses Zustandes wird von der UngestecktseinDetektionseinheit 13 vorgenommen. Hierbei wird über die Masseverbindung am Pin 4 der interfaceeinheit 8 ein Spannungspegel überwacht. Beim Austausch der Funktionseinheit wird diese Masseverbindung unterbrochen und die Ungestecktsein-Detektionseinheit 13 registriert diesen Vorgang als Information. Da bei einem mechanisch oder chemischen Angriff auf das Sicherheitsmodul 100 und für jede Trennung des Sicherheitsmoduls 100 von der Interfaceeinheit 8, die Speicherung dieser Information durch den speziellen batteriegetriebenen Schaltungsaufbau gewährleistet ist, kann eine Auswertung dieser Information zu jeder Zeit erfolgen, falls eine Wiederinbetriebnahme gewünscht ist. Die regelmäßige Auswertung dieses Trennungs- bzw. Ungestecktsein-Signals auf der Leitung 139 der Detektionseinheit 13 ermöglicht es dem Prozessor 120 sensitive Daten zu löschen, ohne jedoch damit die Abrechnungs- und Kundendaten in den NVRAM-Speichern zu verändern. Der momentane Zustand des postalischen Sicherheitsmoduls mit den gelöschten sensitiven Daten kann als Wartungszustand aufgefaßt werden, in welchem in der Regel der Austausch, eine Reparatur oder sonstiges vorgenommen wird. Da die sensitiven Daten der Funktionseinheit gelöscht sind, ist ein Fehler aufgrund einer unsachgemäßen Handhabung des postalischen Sicherheitsmoduls ausgeschlossen. Die sensitiven Daten sind beispielsweise kryptographische Schlüssel. Der Prozessor 120 verhindert im Wartungszustand eine Kernfunktionalität des postalischen Sicherheitsmoduls, welche beispielweise in der Abrechnung und/oder Berechnung eines Sicherheitscodes für die Sicherheitsmarkierung in einem Sicherheitsabdruck besteht.

[0026] Zur Wiederinbetriebnahme wird das postalische Sicherheitsmodul PSM zunächst gesteckt und elektrisch mit der entsprechenden Interfaceeinheit 8 eines Postbearbeitungsgerätes verbunden. Anschließend wird das Gerät eingeschaltet und somit das postalische Sicherheitsmodul wieder mit Systemspannung Us+ versorgt. Aufgrund des speziellen Zustandes muß nun der sachgemäße Einbau des postalischen Sicherheitsmoduls durch ihre Funktionseinheit erneut geprüft werden. Hierfür wird eine zweite Stufe einer Prüfung (dynamische Gestecktsein-Detektion) vorgesehen. Über eine zwischen der ersten Funktionseinheit (Prozessor 120) und der Stromschleife 18 der Interfaceeinheit 8 hergestellten operative Verbindung werden Informationen ausgetauscht, deren fehlerfreie Übermittlung den Beweis für den sachgemäßen Einbau erbringt. Dies ist Voraussetzung für eine erfolgreiche Wiederinbetriebnahme.

[0027] Für den Zustandswechsel in den normalen Betriebszustand ist nun noch eine Reinitialisierung der sensitiven Daten erforderlich. Zwischen dem postalischen Sicherheitsmodul und einer dritten Instanz wird eine Kommunikation vorgenommen, wobei letztere diese sensitiven Daten übermittelt. Nach erfolgreicher Übermittlung wird die UngestecktseinDetektionseinheit 13 zurückgesetzt und das postalische Sicherheitsmodul nimmt wieder seinen normalen Betriebszustand ein. Die Wiederinbetriebnahme ist abgeschlossen.

[0028] Die Figur 2 zeigt ein Blockschaltbild einer Frankiermaschine, die mit einer Chipkarten-Schreib/Leseeinheit 70 zum Nachladen von Änderungsdaten per Chipkarte und mit einer Druckeinrichtung 2, welche von einer Steuereinrichtung 1 gesteuert wird, ausgestattet ist. Die Steuereinrichtung 1 weist eine mit einem

Mikroprozessor 91 mit zugehörigen Speichern 92, 93, 94, 95 ausgestattete Hauptplatine 9 auf.

[0029] Der Programmspeicher 92 enthält ein Betriebsprogramm mindestens zum Drucken und wenigstens sicherheitsrelevante Bestandteile des Programms für eine vorbestimmte Format-Änderung eines Teils der Nutzdaten. Der Arbeitsspeicher RAM 93 dient zur flüchtigen Zwischenspeicherung von Zwischenergebnissen. Der nichtflüchtige Speicher NVM 94 dient zur nichtflüchtigen Zwischenspeicherung von Daten, beispielsweise von statistischen Daten, die nach Kostenstellen geordnet sind. Der Kalender/Uhrenbaustein 95 enthält ebenfalls adressierbare aber nichtflüchtige Speicherbereiche zur nichtflüchtigen Zwischenspeicherung von Zwischenergebnissen oder auch bekannten Programmteilen (beispielsweise für den DES-Algorithmus). Es ist vorgesehen, daß die Steuereinrichtung 1 mit der Chipkarten-Schreib/Leseeinheit 70 verbunden ist, wobei der Mikroprozessor 91 der Steuereinrichtung 1 beispielsweise dazu programmiert ist, die Nutzdaten N aus dem Speicherbereich einer Chipkarte 49 zu deren Anwendung in entsprechende Speicherbereiche der Frankiermaschine zu laden. Eine in einen Einsteckschlitz 72 der Chipkarten-Schreib/Leseeinheit 70 eingesteckte erste Chipkarte 49 gestattet ein Nachladen eines Datensatzes in die Frankiermaschine für mindestens eine Anwendung. Die Chipkarte 49 enthält beispielsweise die Portogebühren für alle üblichen Postbefördererleistungen entsprechend des Tarifs der Postbehörde und ein Postbefördererkennzeichen, um mit der Frankiermaschine ein Stempelbild zugenerieren und entsprechend des Tarifs der Postbehörde die Poststücke freizustempeln.

[0030] Die Steuereinrichtung 1 bildet das eigentliche Meter mit den Mitteln 91 bis 95 der vorgenannten Hauptplatine 9 und umfaßt auch eine Tastatur 88, eine Anzeigeeinheit 89 sowie einen anwendungsspezifischen Schaltkreis ASIC 90 und das Interface 8 für das postalische Sicherheitsmodul PSM 100. Das Sicherheitsmodul PSM 100 ist über einen Steuerbus mit dem vorgenannten ASIC 90 und dem Mikroprozessor 91 sowie über den parallelen µC-Bus mindestens mit den Mitteln 91 bis 95 der Hauptplatine 9 und der mit Anzeigeeinheit 89 verbunden. Der Steuerbus führt Leitungen für die Signale CE, RD und WR zwischen dem Sicherheits-modul PSM 100 und dem vorgenannten ASIC 90. Der Mikroprozessor 91 weist vorzugsweise einen Pin für ein vom Sicherheitsmodul PSM 100 abgegebenes Interruptsignal i, weitere Anschlüsse für die Tastatur 88, eine serielle Schnittstelle SI-1 für den Anschluß der ChipkartenSchreib/Lese-Einheit 70 und eine serielle Schnittstelle SI-2 für den optionalen Anschluß eines MODEMs auf Mittels des MODEMs kann beispielsweise das im nichtflüchtigen Speicher des postalischen Sicherheitsmittels PSM 100 gespeicherte Guthaben erhöht werden.

[0031] Das postalische Sicherheitsmittel PSM 100 wird von einem gesicherten Gehäuse umschlossen. Vor jedem Frankierabdruck wird im postalischen Sicherheitsmodul PSM 100 eine hardwaremäßige Abrechnung durchgeführt. Die Abrechnung erfolgt unabhängig von Kostenstellen. Das postalische Sicherheitsmittel PSM 100 kann intern so ausgeführt sein, wie in der europäischen Anmeldung EP 789 333 A3 näher beschrieben wurde. Es ist vorgesehen, daß der ASIC 90 eine serielle Schnittstellenschaltung 98 zu einem im Poststrom vorschalteten Gerät, eine serielle Schnittstellenschaltung 96 zu den Sensoren und Aktoren der Druckeinrichtung 2, eine serielle Schnittstellenschaltung 97 zur Drucksteuerelektronik 16 für den Druckkopf 4 und eine serielle Schnittstellenschaltung 99 zu einem der Druckeinrichtung 20 im Poststrom nachgeschalteten Gerät aufweist. Der DE 197 11 997 ist eine Ausführungsvariante für die Peripherieschnittstelle entnehmbar, welche für mehrere Peripheriegeräte (Stationen) geeignet ist. Sie trägt den Titel: Anordnung zur Kommunikation zwischen einer Basisstation und weiteren Stationen einer Postbearbeitungsmaschine und zu deren Notabschaltung.

[0032] Die Schnittstellenschaltung 96 gekoppelt mit der in der Maschinenbasis befindlichen Schnittstellenschaltung 14 stellt mindestens eine Verbindung zu den Sensoren 6, 7, 17 und zu den Aktoren, beispielsweise zum Antriebsmotor 15 für die Walze 11 und zu einer Reinigungs- und Dichtstation RDS 40 für den Tintenstrahldruckkopf 4, sowie zum Labelgeber 50 in der Maschinenbasis her Die prinzipielle Anordnung und das Zusammenspiel zwischen Tintenstrahldruckkopf 4 und der RDS 40 sind der DE 197 26 642 C2 entnehmbar, mit dem Titel: Anordnung zur Positionierung eines Tintenstrahldruckkopfes und einer Reinigungs- und Dichtvorrichtung.

Einer der in der Führungsplatte 20 angeordneten Sensoren 7, 17 ist der Sensor 17 und dient zur Vorbereitung der Druckauslösung beim Brieftransport. Der Sensor 7 dient zur Briefanfangserkennung zwecks Druckauslösung beim Brieftransport. Die Transporteinrichtung besteht aus einem Transportband 10 und zwei Walzen 11,11'. Eine der Walzen ist die mit einem Motor 15 ausgestattete Antriebswalze 11, eine andere ist die mitlaufende Spannwalze 11'. Vorzugsweise ist die Antriebswalze 11 als Zahnwalze ausgeführt, entsprechend ist auch das Transportband 10 als Zahnriemen ausgeführt, was die eindeutige Kraftübertragung sichert. Ein Encoder 5, 6 ist mit einer der Walzen 11, 11' gekoppelt. Vorzugsweise sitzt die Antriebswalze 11 mit einem Inkrementalgeber 5 fest auf einer Achse. Der Inkrementalgeber 5 ist beispielsweise als Schlitzscheibe ausgeführt, die mit einer Lichtschranke 6 zusammen wirkt, und gibt über die Leitung 19 ein Encodersignal an die Hauptplatine 9 ab.

Es ist vorgesehen, daß die einzelnen Druckelemente des Druckkopfes innerhalb seines Gehäuses mit einer Druckkopfelektronik verbunden sind und daß der Druckkopf für einen rein elektronischen Druck ansteuerbar ist. Die Drucksteuerung erfolgt auf Basis der Wegsteuerung, wobei der gewählte Stempelversatz berücksichtigt wird, welcher per Tastatur 88 oder bei Bedarf per Chipkarte eingegeben und im Speicher NVM 94 nichtflüchtig gespeichert wird. Ein geplanter Abdruck ergibt sich somit aus Stempelversatz (ohne Drucken), dem Frankierdruckbild und gegebenfalls weiteren Druckbildern für Werbeklischee, Versandinformationen (Wahldrucke) und zusätzlichen editierbaren Mitteilungen. Der nichtflüchtige Speicher NVM 94 weist eine Vielzahl an Speicherbereichen auf. Darunter sind solche, welche die geladenen Portogebührentabellen nichtflüchtig speichern.

Die Chipkarten-Schreib/Leseeinheit 70 besteht aus einem zugehörigen mechanischen Träger für die Mikroprozessorkarte und Kontaktiereinheit 74. Letztere gestattet eine sichere mechanische Halterung der Chipkarte in Lese-Position und eindeutige Signalisierung des Erreichens der Leseposition der Chipkarte in der Kontaktierungseinheit. Die Mikroprozessorkarte mit dem Mikroprozessor 75 besitzt eine einprogrammierte Lesefähigkeit für alle Arten von Speicherkarten bzw. Chipkarten. Das Interface zur Frankiermaschine ist eine serielle

Schnittstelle gemäß RS232-Standard. Die Datenübertragungsrate beträgt min. 1,2 K Baud. Das Einschalten der Stromversorgung erfolgt mittels einem an der Hauptplatine angeschlossenen Schalter 71. Nach Einschalten der Stromversorgung erfolgt eine Selbsttestfunktion mit Bereitschaftsmeldung.

[0033] In der Figur 3 ist eine perspektivische Ansicht der Frankiermaschine von hinten dargestellt. Die Frankiermaschine besteht aus einem Meter 1 und einer Base 2. Letztere ist mit einer Chipkarten-Schreib/ Leseeinheit 70 ausgestattet, die hinter der Führungsplatte 20 angeordnet und von der Gehäuseoberkante 22 zugänglich ist. Nach dem Einschalten der Frankiermaschine mittels dem Schalter 71 wird eine Chipkarte 49 von oben nach unten in den Einsteckschlitz 72 eingesteckt. Ein zugeführter auf der Kante stehender Brief 3, der mit seiner zu bedruckenden Oberfläche an der Führungsplatte anliegt, wird dann entsprechend der Eingabedaten mit einem Frankierstempel 31 bedruckt. Die Briefzuführöffnung wird durch eine Klarsichtplatte 21 und die Führungsplatte 20 seitlich begrenzt. Die Statusanzeige des auf die Hauptplatine 9 des Meters 1 gesteckten Sicherheitsmoduls 100 ist von außen durch eine Öffnung 109 sichtbar.

[0034] Die Figur 4 zeigt ein Blockschaltbild des postalischen Sicherheitsmoduls PSM 100 in einer bevorzugten Variante. Der negative Pol der Batterie 134 ist auf Masse und einen Pin P23 der Kontaktgruppe 102 gelegt. Der positive Pol der Batterie 134 ist über die Leitung 193 mit dem einen Eingang des Spannungsumschalters 180 und die Systemspannung führende Leitung 191 ist mit dem anderen Eingang des Spannungsumschalters 180 verbunden. Als Batterie 134 eignet sich der Typ SL389/P für eine Lebensdauer bis zu 3,5 Jahren oder der Typ SL-386/P für eine Lebensdauer bis zu 6 Jahren bei einem maximalen Stromverbrauch durch das PSM 100. Als Spannungsumschalter 180 kann ein handelsüblicher Schaltkreis vom Typ ADM 8693ARN eingesetzt werden. Der Ausgang des Spannungsumschalters 180 liegt über die Leitung 136 an der Batterieüberwachungseinheit 12 und der Detektionseinheit 13 an. Die Batterieüberwachungseinheit 12 und die Detektionseinheit 13 stehen mit den Pins 1, 2, 4 und 5 des Prozessors 120 über die Leitungen 135, 164 und 137, 139 in Kommunikationsverbindung. Der Ausgang des Spannungsumschalters 180 liegt über die Leitung 136 außerdem am Versorgungseingang eines ersten Speichers SRAM an, der durch die vorhandene Batterie 134 zum nichtflüchtigen Speicher NVRAM einer ersten Technologie wird.
Das Sicherheitsmodul steht mit der Frankiermaschine über den Systembus 115,117, 118 in Verbindung. Der Prozessor 120 kann über den Systembus und ein Modem 83 in Kommunikationsverbindung mit einer entfernten Datenzentrale eintreten. Die Abrechnung wird vom ASIC 150 vollzogen und vom Prozessor 120 überprüft. Die postalischen Abrechnungsdaten werden in nichtflüchtigen Speichern unterschiedlicher Technologie gespeichert.
Die Systemspannung liegt am Versorgungseingang eines zweiten Speichers NV-RAM 114 an. Bei letzterem handelt es sich um einen nichtflüchtigen Speicher NVRAM einer zweiten Technologie, (SHADOWRAM). Diese zweiten Technologie umfaßt vorzugsweise ein RAM und ein EEPROM, wobei letzteres die Dateninhalte bei Systemspannungsausfall automatisch übernimmt. Der NVRAM 114 der zweiten Technologie ist mit den entsprechenden Adress- und Dateneingängen des ASIC's 150 über einen internen Adreß- und Datenbus 112, 113 verbunden.

[0035] Der ASIC 150 enthält mindestens eine Hardware-Abrecheneinheit für die Berechnung der zu speichernden postalischen Daten. In der Programmable Array Logic (PAL) 160 ist eine Zugriffslogik auf den ASIC 150 untergebracht. Der ASIC 150 wird durch die Logik PAL 160 gesteuert. Ein Adreß- und Steuerbus 117, 115 von der Hauptplatine 9 ist an entsprechenden Pins der Logik PAL 160 angeschlossen und die PAL 160 erzeugt mindestens ein Steuersignal für das ASIC 150 und ein Steuersignal 119 für den Programmspeicher FLASH 128. Der Prozessor 120 arbeitet ein Programm ab, das im FLASH 128 gespeichert ist. Der Prozessor 120, FLASH 28, ASIC 150 und PAL 160 sind über einen modulinternen Systembus miteinander verbunden, der Leitungen 110,111,126,119 für Daten-, Adreß- und Steuersignale enthält.
Der Prozessor 120 des Sicherheitsmoduls 100 ist über einen modulinternen Datenbus 126 mit einem FLASH 128 und mit dem ASIC 150 verbunden. Der FLASH 128 wird mit Systemspannung Us+ versorgt. Er ist beispielsweise ein 128 Kbyte- FLASH-Speicher vom Typ AM29F010-45EC. Der ASIC 150 des postalischen Sicherheitsmoduls 100 liefert über einen modulinternen Adreßbus 110 die Adressen 0 bis 7 an die entsprechenden Adreßeingänge des FLASH 128. Der Prozessor 120 des Sicherheitsmoduls 100 liefert über einen internen Adreßbus 111 die Adressen 8 bis 15 an die entsprechenden Adresseingänge des FLASH 128. Der ASIC 150 des Sicherheitsmoduls 100 steht über die Kontaktgruppe 101 des Interfaces 8 mit dem Datenbus 118, mit dem Adreßbus 117 und dem Steuerbus 115 der Hauptplatine 9 in Kommunikationsverbindung.

[0036] Es ist vorgesehen, daß der Prozessor 120 Speicher 122, 124 aufweist, an welche über die Leitung 138 eine Betriebsspannung Ub+ von einer Spannungsüberwachungseinheit 12 zugeführt wird. Insbesondere eine Echtzeituhr RTC 122 und der Speicher RAM 124 werden von einer Betriebsspannung über die Leitung 138 versorgt. Die Spannungsüberwachungseinheit (Battery Observer) 12 liefert außerdem ein Statussignal 164 und reagiert auf ein Steuersignal 135. Der Spannungsumschalter 180 gibt als Ausgangsspannung auf der Leitung 136 für den Battery Observer 12 und Speicher 116 diejenige seiner Eingangsspannungen als Versorgungsspannung weiter, die größer als die andere ist. Durch die Möglichkeit, die beschriebene Schaltung in Abhängigkeit von der Höhe der Spannungen Us+ und Ub+ automatisch mit der größeren von beiden zu speisen, kann während des Normalbetriebs die Batterie 134 ohne Datenverlust gewechselt werden.

[0037] Die Batterie 134 des Sicherheitsmoduls 100 speist in den Ruhezeiten außerhalb des Normalbetriebes in vorerwähnter Weise die Echtzeituhr (RTC) 122 mit Datums und/oder Uhrzeitregistern und/oder den statischen RAM (SRAM) 124, der sicherheitsrelevante Daten hält. Sinkt die Spannung der Batterie während des Batteriebetriebs unter eine bestimmte Grenze, so wird von der Spannungsüberwachungseinheit 12 der Speisepunkt für die RTC und SRAM bis zum Rücksetzen mit Masse verbunden. Die Spannung an der RTC und am SRAM liegt dann bei 0V. Das führt dazu, daß der SRAM 124, der z.B. wichtige kryptografische Schlüssel enthält, sehr schnell gelöscht wird. Gleichzeitig werden auch die Register der RTC 122 gelöscht und die aktuelle Uhrzeit und das aktuelle Datum gehen verloren. Durch

diese Aktion wird verhindert, daß ein möglicher Angreifer durch Manipulation der Batteriespannung die frankiermaschineninterne Uhr 122 anhält, ohne daß sicherheitsrelevante Daten verloren gehen. Somit wird verhindert, daß der Angreifer Sicherheitsmaßnahmen, wie beispielsweise Long Time Timer oder Watchdogs umgeht. Die vorgenannten Sicherheitsmaßnahmen werden anhand der Figuren 9 und 10 ausführlich erläutert.

[0038] Die RESET-Einheit 130 ist über die Leitung 131 mit dem Pin 3 des Prozessors 120 und mit einem Pin des ASIC's 150 verbunden. Der Prozessor 120 und das ASIC 150 werden bei Absinken der Versorgungsspannung durch eine Resetgenerierung in der RESET-Einheit 130 zurückgesetzt.

[0039] Gleichzeitig mit der Indikation der Unterspannung der Batterie wechselt die beschriebene Schaltung in einen Selbsthaltezustand, in dem sie auch bei nachträglicher Erhöhung der Spannung bleibt. Beim nächsten Einschalten des Moduls kann der Prozessor den Zustand der Schaltung abfragen (Statussignal) und damit und/oder über die Auswertung der Inhalte des gelöschten Speichers darauf schließen, daß die Batteriespannung zwischenzeitlich einen bestimmten Wert unterschritten hat. Der Prozessor kann die Überwachungsschaltung zurücksetzen, d.h. "schart" machen.

[0040] Die Ungestecktsein-Detektionseinheit 13 hat zur Messung der Eingangsspannung eine Leitung 192, die über den Stecker des Sicherheitsmoduls und Interface 8, vorzugsweise über einen Sockel auf der Mutterplatine 9 der Frankiermaschine mit Masse verbunden ist. Diese Messung dient zur statischen Überwachung des Gesteckseins und bildet die Grundlage für eine Überwachung auf einer ersten Stufe. Es ist vorgesehen, daß die Ungestecktsein-Detektionseinheit 13 Schaltungsmittel für eine rücksetzbare Selbsthaltung aufweist, wobei die Selbsthaltung ausgelöst wird, wenn der Spannungspegel auf einer Meßspannungsleitung 192 von einem vorbestimmten Potential abweicht. Zugleich umfaßt die AuswerteLogik den mit den anderen Funktionseinheiten verbundenen Prozessor 120, welcher programmiert ist, den jeweiligen Zustand des Sicherheitsmoduls 100 festzustellen und zu verändern. Der Zustand der Selbsthaltung ist über die Leitung 139 vom Prozessor 120 des Sicherheitsmoduls 100 abfragbar. Das Meßspannungspotential auf der Leitung 192 entspricht Massepotential, wenn der Sicherheitsmodul 100 ordnungsgemäß gesteckt ist. Auf der Leitung 139 liegt Betriebsspannungspotential. Massespannungspotential liegt auf der Leitung 139 an, wenn der Sicherheitsmodul 100 ungesteckt ist. Der Prozessor 120 weist einen fünften Pin5 auf, an welchem die Leitung 139 angeschlossen ist, um den Zustand der Ungestecktsein-Detektionseinheit 13 abzufragen, ob sie auf Massepotential mit Selbsthaltung geschaltet ist. Um den Zustand der Selbsthaltung der Ungestecktsein-Detektionseinheit 13 über die Leitung 137 zurückzusetzen, weist der Prozessor 120 einen vierten Pin 4 auf.

[0041] Weiterhin ist eine Stromschleife 18 vorgesehen, die die Pins 6 und 7 des Prozessors 120 ebenfalls über den Stecker des Sicherheitsmoduls und über den Sockel auf der Hauptplatine 9 der Frankiermaschine miteinander verbindet. Die Leitungen an den Pins 6 und 7 des Prozessors 120 sind nur bei einem an die Hauptplatine 9 gesteckten PSM 100 zu einer Stromschleife 18 geschlossen. Diese Schleife bildet die Grundlage für eine dynamische Überwachung des Angestecktseins des Sicherheitsmoduls auf einer zweiten Stufe.

[0042] Der Prozessor 120 weist intern eine Verarbeitungseinheit CPU 121, eine Echtzeituhr RTC 122 eine RAM-Einheit 124 und eine Ein/Ausgabe-Einheit 125 auf Der Prozessor 120 ist mit Pin's 8, 9 zur Ausgabe mindestens eines Signals zur Signalisierung des Zustandes des Sicherheitsmoduls 100 ausgestattet. An den Pins 8 und 9 liegen I/O-Ports der Ein/AusgabeEinheit 125, an welchen modulinterne Signalmittel angeschlossen sind, beispielsweise farbige Lichtemitterdioden LED's 107, 108, welche den Zustand des Sicherheitsmoduls 100 signalisieren. Die Sicherheitsmodule können in ihrem Lebenszyklus verschiedene Zustände einnehmen. So muß z.B. detektiert werden, ob das Modul gültige kryptografische Schlüssel enthält. Weiterhin ist es auch wichtig zu unterscheiden, ob das Modul funktioniert oder defekt ist. Die genaue Art und Anzahl der Modulzustände ist von den realisierten Funktionen im Modul und von der Implementierung abhängig.

[0043] Anhand der Figur 5 wird das Schaltbild der Detektionseinheit 13 erläutert. Es ist vorgesehen, daß die Ungestecktsein-Detektionseinheit 13 einen Spannungsteiler aufweist, der aus einer Reihenschaltung von Widerständen 1310, 1312, 1314 besteht und zwischen einem von einem Kondensator 1371 abgreifbaren Versorgungsspannungspotential und einem Meßspannungspotential auf der Leitung 192 gelegt ist. Die Schaltung wird über die Leitung 136 mit der System- oder Batteriespannung versorgt. Die jeweilige Versorgungsspannung von der Leitung 136 gelangt über eine Diode 1369 auf den Kondensator 1371 der Schaltung. Ausgangsseitig der Schaltung liegt ein Negator 1320, 1398. Im Normalzustand ist der Transistor 1320 des Negators gesperrt und die Versorgungsspannung wird über den Widerstand 1398 auf der Leitung 139 wirksam, welche deshalb logisch '1', d.h. H-Pegel im Normalzustand führt. Ein L-Pegel auf der Leitung 139 ist vorteilhaft als Statussignal für ein Ungestecktsein, weil dann in den Pin 5 des Prozessors 120 kein Strom hineinfließt, was die Batterielebensdauer erhöht. Die Diode 1369 sorgt vorzugsweise in Zusammenhang mit einem Elektrolytkondensator 1371 dafür, daß die dem Negator vorgeschaltete Schaltung über einen relativ langen Zeitraum (>2 s) mit einer Spannung versorgt wird, bei der deren Funktion gewährleistet ist, obwohl die Spannung auf der Leitung 136 bereits abgeschaltet wurde.

Der Spannungsteiler 1310, 1312, 1314 weist einen Abgrift 1304 auf, an welchem ein Kondensator 1306 und der nichtinvertierende Eingang eines Komparators 1300 angeschlossen sind. Der invertierende Eingang des Komparators 1300 ist mit einer Referenzspannungsquelle 1302 verbunden. Der Ausgang des Komparators 1300 ist einerseits über den Negator 1324,1398 mit der Leitung 139 und andererseits mit dem Steuereingang eines Schaltmittels 1322 für die Selbsthaltung verbunden. Das Schaltmittel 1322 ist zum Widerstand 1310 des Spannungsteilers parallel geschaltet und das Schaltmittel 1316 für eine Rücksetzung der Selbsthaltung ist zwischen dem Abgriff 1304 und Masse geschaltet. Der Abgriff 1304 des Spannungsteilers liegt am Verbindungspunkt der Widerstande 1312 und 1314. Der zwischen dem Abgriff 1304 und Masse geschaltete Kondensator 1306 verhindert Schwingungen. Die Spannung am Abgriff 1304 des Spannungsteilers wird im Komparator 1300 mit der Referenzspannung der Quelle 1302 verglichen. Ist die zu vergleichende Spannung am Abgriff 1304 kleiner als die Referenzspannung der Quelle 1302, 50 bleibt der Komparatorausgang auf L-Pegel geschaltet und der Transistor 1320 des Negators ist gesperrt. Dadurch erhält die

Leitung 139 nun Betriebsspannungspotential und das Statussignal führt logisch '1'. Der Spannungsteiler ist so dimensioniert, daß bei Massepotential auf der Leitung 192 der Abgriff 1304 eine Spannung führt, welche sicher unterhalb der Schaltschwelle des Komparators 1300 liegt. Wird die Verbindung unterbrochen und die Leitung 192 ist nicht mehr mit Masse verbunden, weil das Sicherheitsmodul 100 vom Sockel auf der Hauptplatine 9 bzw. Interfaceeinheit 8 der Frankiermaschine gelöst wurde, so wird die Spannung am Abgriff 1304 über die Spannung der Referenzspannungsquelle 1302 gezogen und der Komparator 1300 schaltet um. Der Komparatorausgang wird auf H-Pegel geschaltet und folglich ist der Transistor 1320 durchgeschaltet. Dadurch wird die Leitung 139 mit Massepotential verbunden und das Statussignal führt logisch '0. Mit Hilfe eines Transistors 1322, welcher dem Widerstand 1310 des Spannungsteilers parallelgeschaltet ist, wird eine Selbsthalteschaltung der Ungestecktsein-Detektionseinheit 13 realisiert. Der Steuereingang des Transistors 1322 wird vom Komparatorausgang auf H-Pegel geschaltet. Dadurch schaltet der Transistor 1322 durch und überbrückt den Widerstand 1310. Infolgedessen wird der Spannungsteiler nur noch durch die Widerstände 1312 und 1314 gebildet. Dadurch wird die Umschaltschwelle so weit erhöht, daß der Komparator auch im geschalteten Zustand bleibt, wenn die Leitung 192 wieder Massepotential führt, weil das Sicherheitsmodul wieder gesteckt wurde.

Der Zustand der Schaltung kann über das Signal auf der Leitung 139 vom Prozessor 120 abgefragt werden.

Es ist vorgesehen, daß die Ungestecktsein-Detektionseinheit 13 als Schaltungsmittel eine Leitung 137 und ein Schaltmittel 1316 für eine Rücksetzung der Selbsthaltung aufweist, wobei die Rücksetzung vom Prozessor 120 über ein Signal auf der Leitung 137 auslösbar ist. Der Prozessor 120 kann jederzeit über einen Anwenderschaltkreis ASIC 150, über eine erste Kontaktgruppe 101, über einen Systembus der Steuereinrichtung 1 und beispielsweise über den Mikroprozessor 91 per Modem 83 den Kontakt zu einer entfernten Datenzentrale aufnehmen, welche die Abrechnungsdaten überprüft und gegebenenfalls weitere Daten an den Prozessor 120 übermittelt. Der Anwenderschaltkreis ASIC 150 des Sicherheitsmoduls 100 ist mit dem Prozessor 120 über einen modulinternen Datenbus 126 verbunden.

Der Prozessor 120 kann die Ungestecktsein-Detektionseinheit zurücksetzen, wenn mittels der übermittelten Daten eine Reinitialisation erfolgreich abgeschlossen werden konnte. Dazu wird über das Rücksetzsignal auf der Leitung 137 der Transistor 1316 durchgeschaltet und somit die Spannung am Abgriff 1304 unter die Referenzspannung der Quelle 1302 gezogen und die Transistoren 1320 und 1322 sperren. Ist der Transistor 1322 im Normalzustand gesperrt, so bilden die Widerstände 1310 und 1312 in Serie den oberen Teil des oben genannten Spannungsteilers und die Umschaltschwelle wird wieder auf den Ursprungszustand abgesenkt.

[0044] Die Figur 6 zeigt zeigt den mechanischen Aufbau des Sicherheitsmoduls in Seitenansicht. Das Sicherheitsmodul ist als Multi-Chip-Modul ausgebildet, d.h. mehrere Funktionseinheiten sind auf einer Leiterplatte 106 verschaltet. Das Sicherheitsmodul 100 ist mit einer harten Vergußmasse 105 vergossen, wobei die Batterie 134 des Sicherheitsmoduls 100 außerhalb der Vergußmasse 105 auf einer Leiterplatte 106 auswechselbar angeordnet ist. Beispielsweise ist es so mit einem Vergußmaterial 105 vergossen, daß Signalmittel 107, 108 aus dem Vergußmaterial an einer ersten Stelle herausragen und daß die Leiterplatte 106 mit der gesteckten Batterie 134 seitlich einer zweiten Stelle herausragt. Die Leiterplatte 106 hat außerdem Batteriekontaktklemmen 103 und 104 für den Anschluß der Pole der Batterie 134, vorzugsweise auf der Bestückungsseite oberhalb der Leiterplatte 106. Es ist vorgesehen, daß zum Anstecken des postalischen Sicherheitsmoduls PSM 100 auf die Hauptplatine des Meters 1 die Kontaktgruppen 101 und 102 unterhalb der Leiterplatte 106 (Leiterbahnseite) des Sicherheitsmoduls 100 angeordnet sind. Der Anwenderschaltkreis ASIC 150 steht über die erste Kontaktgruppe 101 - in nicht gezeigter Weise - mit dem Systembus einer Steuereinrichtung 1 in Kommunikationsverbindung und die zweite Kontaktgruppe 102 dient der Versorgung des Sicherheitsmoduls 100 mit der Systemspannung. Wird das Sicherheitsmodul auf die Hauptplatine gesteckt, dann ist es vorzugsweise innerhalb des Metergehäuses dergestalt angeordnet, so daß das Signalmittel 107, 108 nahe einer Öffnung 109 ist oder in diese hineinragt. Das Metergehäuse ist damit vorteilhaft so konstruiert, daß der Benutzer die Statusanzeige des Sicherheitsmoduls trotzdem von außen sehen kann. Die beiden Leuchtdioden 107 und 108 des Signalmittels werden über zwei Ausgangssignale der I/O-Ports an den Pin 8, 9 des Prozessors 120 gesteuert. Beide Leuchtdioden sind in einem gemeinsamen Bauelementegehäuse untergebracht (Bicolorleuchtdiode), weshalb die Abmaße bzw. der Durchmesser der Öffnung relativ klein bleiben kann und in der Größenordnung des Signalmittels liegt. Prinzipiell sind drei unterschiedliche Farben darstellbar (rot, grün, orange). Zur Zustandsunterscheidung werden die LED's auch blinkend benutzt, so daß 8 verschiedene Zustandsgruppen unterschieden werden können, die durch folgende LED-Zustände charakterisiert werden: LED grün leuchtend, LED rot leuchtend, LED Orange leuchtend, LED rot blinkend, LED grün blinkend, LED orange blinkend, LED rot leuchtend und orange blinkend sowie LED grün leuchtend und orange blinkend.

[0045] In der Figur 7 ist eine Draufsicht auf das postalische Sicherheitsmodul dargestellt.

[0046] Die Figuren 8a bzw. 8b zeigen eine Ansicht des Sicherheitsmoduls jeweils von rechts bzw. von links. Die Lage der Kontaktgruppen 101 und 102 unterhalb der Leiterplatte 106 wird aus den Figuren 8a und 8b in Verbindung mit Figur 6 deutlich.

[0047] Gemäß einer in der Figur 9 gezeigten - sich selbst erläuternden - Tabelle für Statussignalisierung geht eine Vielzahl möglicher Zustandsanzeigen hervor. Eine grün leuchtende LED 107 signalisiert einen OK-Zustand 220, aber eine leuchtende LED 108 signalisiert einen Fehler-Zustand 230 im Ergebnis eines mindestens statischen Selbsttestes. Das Ergebnis eines solchen an sich bekannten Selbsttestes kann wegen der direkten Signalisierung über die LED's 107,108 nicht verfälscht werden. Beispielsweise für den Fall, daß zwischenzeitlich die im Sicherheitsmodul gespeicherten Schlüssel verlohren gingen, würde die laufende Überprüfung im dynamischen Betrieb den Fehler feststellen und als den Zustand 240 mit orange leuchtenden LED's signalisieren. Nach einem Aus/Einschalten ist ein Booten erforderlich, da anderenfalls keine andere Operation mehr ausgeführt werden kann. Der Fall, daß bei der Herstellung die Installation eines Schlüssels vergessen wurde, wird als Zustand 260 beispielsweise mit einer grün

blinkenden LED 107 signalisiert.

Die erste Funktionseinheit ist der Prozessor 120. Dieser wertet ständig einen zweiten Tageskredit daraufhin aus, ob letzterer erschöft ist. Das ist der Fall, wo ein long time Timer abgelaufen ist. Der long time Timer ist abgelaufen, wenn eine zu lange Zeit die Datenzentrale nicht mehr kontaktiert wurde, beispielsweise dazu um ein Guthaben nachzuladen. Als Zeitkredit können von der Datenzentrale beispielsweise 90 Tage vorgegeben und bei der Installation oder beim Nachladen in einen Speicher 124 des Sicherheitsgerätes geladen werden. Nach Ablauf dieser 90 Tage wird ein „LOST" -Zustand 250 durch eine rot blinkende LED signalisiert. Der long time Timer ist vorzugsweise ein Rückwärtszähler, der im Prozessor 120 realisiert wird. Da bei Zeitablauf der Zählerstand Null erreicht wird bleibt der Zustand 250 ebenfalls bestehen, wenn das Sicherheitsmodul vom Meter getrennt wurde, nachdem der „LOST"Zustand erreicht wurde. Wenn der letzte Kontakt zur Datenzentrale solange zurückliegt, daß dies bereits verdächtig erscheint, wird der suspekte Zustand 270 signalisiert, vorzugsweise ein Rückwärtszähler, der ebenfalls im Prozessor 120 realisiert ist, der ständig einen ersten Tageskredit von beispielsweise 30 Tagen daraufhin auswertet, ob letzterer erschöft ist.

[0048] Weitere Zustandsanzeigen für die Zustände 280 und 290 sind optional für verschiedene weitere Prüfungen vorgesehen. Dazu können weitere Funktionseinheiten, insbesondere ein Temperaturfühler, im Sicherheitsmodul vorgesehen sein. Wurde zum Beispiel eine Temperatur überschritten, welche zu Schäden im Sicherheitsmodul führen konnte, so kann dieser Zustand 280 mit den LED's 107, 108 signalisiert werden, die rot leuchten und orange blinken und somit die Gesamtwirkung des abwechselnd rot/orange Blinkens hervorrufen. Die zweite Funktionseinheit kann die Batteriespannung gegebenenfalls daraufhin überwachen, ob deren Kapazität erschöpft ist. Vorteilhaft kann ein Zustand 290 für einen erforderlichen Batteriewechsel mit den LED's 107, 108 signalisiert werden, die grün leuchten und orange blinken und somit die Gesamtwirkung des abwechselnd grün/orange Blinkens hervorrufen.

[0049] Die Figur 10 zeigt eine Darstellung der Prüfungen im System für statisch und dynamisch änderbare Zustände. Ein ausgeschaltetes System im Zustand 200 geht nach dem Einschalten über die Transition Start 201 in den Zustand 210 über, in welchem vom Sicherheitsmodule ein statischer Selbsttest durchgeführt wird sobald die Betriebsspannung anliegt. Bei der Transition 202, bei der der Selbsttest ein OK bei ordnungsgemäßem Ergebnis ergibt, wird der Zustand 220 mit LED 107 grün leuchtend erreicht. Ausgehend von letzterem Zustand sind bei Bedarf ein wiederholter statischer Selbsttest, ein dynamischer Dauer-Test, mindestens ein periodischer Zeitkredit-Test und andere Teste durchführbar. Eine solche Tests veranschaulichende Transition 203 führt zurück auf den Zustand 220 LED grün bei OK. Eine Transition 206 führt auf den Zustand 240 und die LED's leuchten orange bei einem während des dynamischen Selbsttest festgestellten Fehler. Letzterer ist durch einen Recover-Versuch evtl. durch Ausschalten (Transition 211) und Wiedereinschalten des Gerätes (Transition 201) behebbar. Statische Fehler sind aber nicht behebbar. Vom Zustand 210, in welchem das eingeschaltete Gerät einen statischen Selbsttest ausführt, existiert bei einem Fehler eine Transition 204 zum Zustand 230 und die LED 108 leuchtet rot. Zu jeder Zeit, wenn sich das Gerät im Zustand 220 (LED grün) befindet, kann ein on demand ausgeführter statischer Selbsttest bei einem Fehler über eine Transition 205 zum Zustand 230 (LED rot) führen. Ausgehend vom Zustand 220 (LED grün) führen weitere Transitionen 207, 208, 209 zu den weiteren Zuständen 270, 250, 260. Im Zustand 270 wird mit orange blinkenden LED's 107, 108 signalisiert, daß die Verbindung zur Datenzentrale aufgenommen werden soll, da das Sicherheitsgerät bereits als suspekt gilt. Über die Transition 212, die das Nachladen ergibt, wird wieder der Zustand 210 erreicht.

Im Zustand 250 wird mit der rot blinkenden LED 108 der Zustand „LOST" signalisiert. Bei der Transition 209 bei der ein weiterer Selbsttest des Prozessors 120 ein Erfordernis des Nachladens eines Schlüssels ergibt, wird der Zustand 260 mit LED 107 grün blinkend erreicht.

Ausgehend vom Zustand 220 (LED 107 grün) können optionale weitere Transitionen entweder zu dem weiteren Zustand 280 mit rot leuchtend/orange blinkenden LED's oder dem Zustand 290 mit grün leuchtend/orange blinkenden LED's führen. Bei der ersten optionalen Transition ergibt eine Temperaturmessung ein Erfordernis des Auswechseins des ganzen Sicherheitsmoduls. Bei der letzteren Transition ergibt eine Kapazitätsmessung der Batterie ein Erfordernis des Batteriewechselns.

[0050] Die Figur 11 zeigt zeigt den mechanischen Aufbau des Sicherheitsmoduls nach einer zweiten Variante in Seitenansicht. Das Sicherheitsmodul ist wieder als Multi-Chip-Modul ausgebildet und mit einer harten Vergußmasse 105 vergossen, wobei die Batterie 134 des Sicherheitsmoduls 100 außerhalb der Vergußmasse 105 auf einer Leiterplatte 106 auswechselbar angeordnet ist. Aus Kostengründen erfolgt der Verguß an einer ersten Stelle so mit einem Vergußmaterial 105, dass das Signalmittel 107, 108 und die gesteckte Batterie 134 extern vom Vergußmaterial an einer zweiten Stelle auf der Oberseite der Leiterplatte 106 montiert sind. Die Leiterplatte 106 hat wieder Batteriekontaktklemmen 103 und 104 für den Anschluß der Pole der Batterie 134, vorzugsweise auf der Bestückungsseite oberhalb der Leiterplatte 106. Die beiden Leuchtdioden 107 und 108 des Signalmittels sind bei dieser Variante separate Bauelemente. Die beiden Leuchtdioden 107 und 108 des Signalmittels werden über zwei Ausgangssignale der I/O-Ports an den Pin 8, 9 des Prozessors 120 gesteuert. Zur Zustandsunterscheidung können die LED's wiederum auch blinkend gesteuert werden, so daß verschiedene Zustandsgruppen unterschieden werden können. Das Metergehäuse ist ebenfalls wieder so konstruiert, daß der Benutzer die Statusanzeige des Sicherheitsmoduls von außen, beispielsweise durch ein Sichtfenster oder eine Öffnung 109 sehen kann.

Es ist ebenfalls vorgesehen, dass zum Anstecken des postalischen Sicherheitsmoduls PSM 100 auf die Hauptplatine des Meters 1 die Kontaktgruppen 101 und 102 unterhalb der Leiterplatte 106 des Sicherheitsmoduls 100 angeordnet sind. Vorteilhaft enthält ein Verbinder 127 die Kontaktgruppen 101 und 102, wobei ein Verbinder 127 auf der Leiterbahnseite der Leiterplatte 106 angeordnet ist.

[0051] In der Figur 12 ist eine Draufsicht auf das postalische Sicherheitsmodul der zweiten Variante dargestellt. Die Vergußmasse 105 umgibt quaderförmig den ersten Teil der Leiterplatte 106, während der zweite Teil der Leiterplatte 106 für die beiden Leuchtdioden 107 und 108, die auswechselbar angeordnete Batterie 134 und für den

Verbinder 127 (hier nicht sichtbar) frei von Vergußmasse bleibt. Die Batteriekontaktklemmen 103 und 104 werden in der Figur 12 von der Batterie verdeckt, sind aber ebenso wie der Verbinder 127 in der Seitenansicht nach Fig.13a sichtbar.

[0052] Der Verguß des ersten Teils der Leiterplatte 106 zeigt weder Öffnungen noch Erhebungen und bietet somit weniger Angriffspunkte für ein Manipulation in krimineller Absicht. Das Vergußmaterial 105 ist vorzugsweise ein Zweikomponenten-Epoxitharz oder Polymer bzw. Kunststoff. Geeignet ist eine Vergußmasse aus STYCAST ®2651-40 FR von der Firma EMERSON & CUMING mit vorzugsweise CATALYST 9 als zweite Komponente. Bei der Herstellung des Vergusses werden beide Komponenten gemischt und auf beide Seiten der Leiterplatte 106 in deren ersten Teil aufgebracht. Letzteres kann beispielsweise durch Eintauchen in die frische Mischung erfolgen. Nun kann eine - nach einem abschließend äusserem Verguß von aussen nicht sichtbare - Schutz-und/oder Sensorschicht angebracht werden, welche während des Aushärtens des Vergußmaterials 105 mit letzterem eine feste Verbindung eingeht. Nach dem abschließenden äusseren Verguß härtet die Vergussmasse zu dem festen undurchsichtigen Vergußmaterials 105 aus.

[0053] Die Figuren 13a bzw. 13b zeigen eine Ansicht des Sicherheitsmoduls der zweiten Variante jeweils von rechts bzw. von links. Die Lage des Verbinders 127 mit den Kontaktgruppen 101 und 102 unterhalb der Leiterplatte 106 wird aus den Figuren 13a und 13b in Verbindung mit Figur 12 deutlicher sichtbar.
Alternativ kann beispielsweise ein Verbinder 127 - in nicht gezeigter Weise - auf der Oberseite des zweiten Teils der Leiterplatte 106 angebracht werden.

[0054] Prinzipiell kann natürlich auch ein anderes Signalmittel in Verbindung mit einem postalischen Gerät eingesetzt werden.
Erfindungsgemäß ist das postalische Gerät, insbesondere eine Frankiermaschine. Das Sicherheitsmodul kann dann als postalisches Sicherheitsgerät PSD (POSTAL SECURITY DEVICE) durch die jeweilige Postbehörde zugelassen werden.

[0055] Das Sicherheitsmodul bzw. PSD auch eine andere Bauform aufweisen, die es ermöglicht, daß es beispielsweise auf die Hauptplatine eines Personalcomputers gesteckt werden kann, der als PC-Frankierer einen handelsüblichen Drucker ansteuert.

[0056] Die Erfindung ist nicht auf die vorliegenden Ausführungsform beschränkt, da offensichtlich weitere andere Anordnungen bzw. Ausführungen der Erfindung entwickelt bzw. eingesetzt werden können, die - vom gleichen Grundgedanken der Erfindung ausgehend - von den anliegenden Ansprüchen umfaßt werden.

Patentansprüche

1. Verfahren zum Schutz eines Sicherheitsmoduls, mit den folgenden Schritten:

   - Überwachung des Zustandes, des sachgemäßen Gebrauchs oder Austausches des Sicherheitsmoduls mindestens mittels zweier Funktionseinheiten (120, 12, 13),
   - Signalisieren mindestens eines Zustandes (220, 230, 240, 250, 260, 270, 280, 290) gesteuert mittels einer ersten Funktionseinheit (120) und
   - Löschen von sensitiven Daten aufgrund eines unsachgemäßen Gebrauchs oder Austausches mindestens mittels einer zweiten Funktionseinheit (12).

2. Verahren, nach Ansprunch 1, **gekennzeichnet dadurch**, daß mittels der ersten Funktionseinheit (120) ein Zeitablauf detektiert wird und daß zur Wiederherstellung der Funktionen ein weiterer Verfahrensablauf erfolgt, mit den Schriften:

   - Reinitialisieren mittels der ersten Funktionseinheit (120) von zuvor gelöschten sensitiven Daten nach sachgemäßem Gebrauch oder Austausch des Sicherheitsmoduls, und
   - Wiederinbetriebnahme durch Freischalten der Funktionseinheiten (12, 13) des Sicherheitsmodules (100).

3. Verfahren, nach Anspruch 1, **gekennzeichnet dadurch**, daß mittels der zweiten Funktionseinheit (12) eine Überwachung des sachgemäßen Einsatzes oder Zustandes der Batterie (134) vorgenommen wird.

4. Verfahren, nach Anspruch 1, **gekennzeichnet dadurch**, daß ein Sperren der Funktionalität mittels einer dritten Funktionseinheit (13) aufgrund eines Austausches des Sicherheitsmoduls oder aufgrund eines Zerstörungszustandes nach einem Angriff erfolgt.

5. Verfahren, nach Anspruch 4, **gekennzeichnet dadurch**, daß mittels der dritten Funktionseinheit (13) ein Zerstörungszustand nach einem mechanischen oder chemischen Angriff detektiert wird

6. Verfahren, nach Anspruch 2, **gekennzeichnet dadurch**, daß die erste Funktionseinheit ständig einen ersten Tageskredit auswertet, wobei ein suspekter Zustand signalisiert wird, wenn der Tageskredit erschöft ist.

7. Verfahren, nach Anspruch 6, **gekennzeichnet dadurch**, daß durch eine Kontaktaufnahme mit der Datenzentrale der normale Arbeitszustand wiederhergestellt werden, ohne daß eine Inspektion vor Ort durch einen Service erforderlich wird.

8. Verfahren, nach Anspruch 2, **gekennzeichnet dadurch**, daß der Zeitkredit variabel und von Sicherheitsgerät zu Sicherheitsgerät unterschiedlich ist und bei der Installation in einen Speicher des Sicherheitsgerätes geladen werden kann.

9. Verahren, nach Anspruch 2, **gekennzeichnet dadurch**, daß die erste Funktionseinheit (120) ständig einen zweiten Tageskredit auswertet, welcher länger als der erste Tageskredit läuft, wobei der Zustand "LOST" signalisiert wird, wenn der zweite Tageskredit erschöft ist.

10. Anordnung zur Durchführung des Verfahrens nach Anspruch 1, wobei ein Sicherheitsmodul, mit einer Logik (120, 150, 160), Mitteln zur Versorgung des Sicherheitsmoduls mit einer Systemspannung oder mit einer Spannung aus einer Batterie (134) und mit einer Anzahl an Überwachungsmitteln ausgestattet ist, **gekennzeichnet** durch mindestens eine erste (120) und zweite Funktionseinheit (12) sowie durch Mittel zum Laden mindestens eines von der Datenzentrale vorgegebenen Zeitkredits und durch ein Signalmittel (107, 108), welches mit einer ersten Funktionseinheit (120) verbunden ist, wobei das Laden bei der Installation und beim Nachladen in einen Speicher (124) des Sicherheitsgerätes vorgenommen wird, und wobei die erste Funktionseinheit (120) einen Tageskredit auf Zeitablauf auswertet und das Signalmittel (107, 108) ansteuert, mindestens um den Zeitablauf zu signalisieren, sowie durch Mittel der zweiten Funktionseinheit (12) zum Löschen von sensitiven Daten im Speicher (124) aufgrund eines unsachgemäßen Gebrauchs oder Austausches des Sicherheitsmoduls.

11. Anordnung, nach Anspruch 10, **gekennzeichnet dadurch**, daß die zweite Funktionseinheit (12) eine Spannungsüberwachungseinheit (12) ist, welche über eine Leitung (136) mit Mitteln zur Versorgung des Sicherheitsmoduls mit einer Systemspannung oder mit einer Batteriespannung verbunden ist, wobei die die zweite Funktionseinheit (12) über eine Leitung (138) eine Betriebsspannung an einen Speicher (122, 124) abgibt.

12. Anordnung, nachAnspruch 10, **gekennzeichnet dadurch**, daß eine dritte Funktionseinheit (13) eine Detektionseinheit mit Schaltungsmitteln (1310, 1316, 1322, 1324) für eine rücksetzbare Selbsthaltung vorhanden ist, wobei die Selbsthaltung ausgelöst wird, wenn der Spannungspegel auf einer Meßspannungsleitung (192) von einem vorbestimmten Potential abweicht und daß der mit den Funktionseinheiten (12, 13) verbundene Prozessor (120) programmiert ist, den jeweiligen Zustand des Sicherheitsmoduls (100) festzustellen und zu signalisieren.

13. Anordnung, nach den Ansprüchen 10 bis 12, **gekennzeichnet dadurch**, daß der Prozessor (120) Speicher (122, 124) aufweist, an welche über die Leitung (138) eine Betriebsspannung Ub+ von einer Spannungsüberwachungseinheit (12) geführt wird, daß der Prozessor (120) mit Systemspannung Us+ versorgt wird und einen vierten Anschluß (Pin 4) aufweist, um den Zustand der Selbsthaltung der Detektionseinheit (13) über die Leitung (137) zurückzusetzen und einen fünften Anschluß (Pin 5) aufweist, an welchem die Leitung (139) angeschlossen ist, um den Zustand der Detektionseinheit (13) abzufragen.

14. Anordnung, nach einem der Ansprüche 10 bis 13, **gekennzeichnet dadurch**, daß das Sicherheitsmodul (100) mit einer harten Vergußmasse (105) vergossen ist, daß die Batterie (134) des Sicherheitsmoduls (100) außerhalb der Vergußmasse (105) auf einer Leiterplatte (106) auswechselbar angeordnet ist, daß die Leiterplatte (106) die Batteriekontaktklemmen (103 und 104) für den Anschluß der Pole der Batterie (134) und eine zweite Kontaktgruppe (102) zur Versorgung des Sicherheitsmoduls (100) mit der Systemspannung aufweist und daß die Vergußmasse mit Mitteln ausgestattet sind, welche des Sicherheitsmodul (100) vor einem Angriff warnen und ggf. schützen sowie daß mindestens eine der Kontaktgruppen (101, 102) zur statischen und dynamischen Überwachung des Angestecktseins und des Angegriffenseins des Sicherheitsmoduls (100) ausgebildet ist.

15. Anordnung, nach einem der Ansprüche 10 bis 14, **gekennzeichnet dadurch**, daß der Prozessor (120) des Sicherheitsmoduls mit Anschlüssen (Pin's 8, 9) zur Ausgabe mindestens eines Signals zur Signalisierung des Zustandes des Sicherheitsmoduls (100) ausgestattet ist.

16. Anordnung, nach Anspruch 15, **gekennzeichnet dadurch**, daß an den I/O-Ports einer Ein/Ausgabe-Einheit (125) des Prozessors (120) modulinterne Signalmittel (107,108) angeschlossen sind.

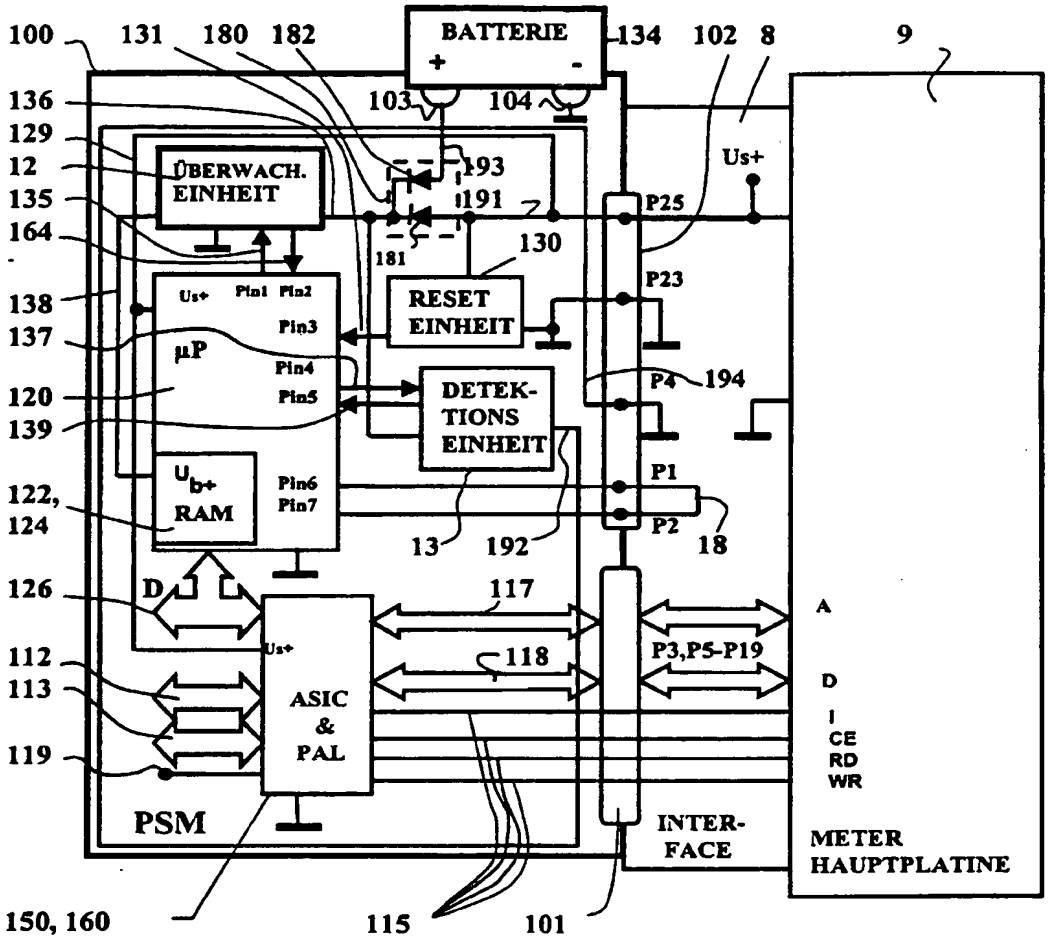

100
131
180
182
BATTERIE
+
-
134
102
8
9
136
103
104
129
12
ÜBERWACH.
EINHEIT
193
Us+
135
191
P25
164
181
130
RESET
EINHEIT
P23
138
Us+
Pin1
Pin2
Pin3
137
µP
Pin4
Pin5
DETEK-
TIONS
EINHEIT
P4
194
120
139
Ub+
RAM
Pin6
Pin7
P1
122,
124
P2
18
13
192
126
D
117
A
112
Us+
118
P3,P5-P19
113
ASIC
&
PAL
D
I
CE
RD
WR
119
PSM
INTER-
FACE
METER
HAUPTPLATINE
150, 160
115
101

Fig. 1

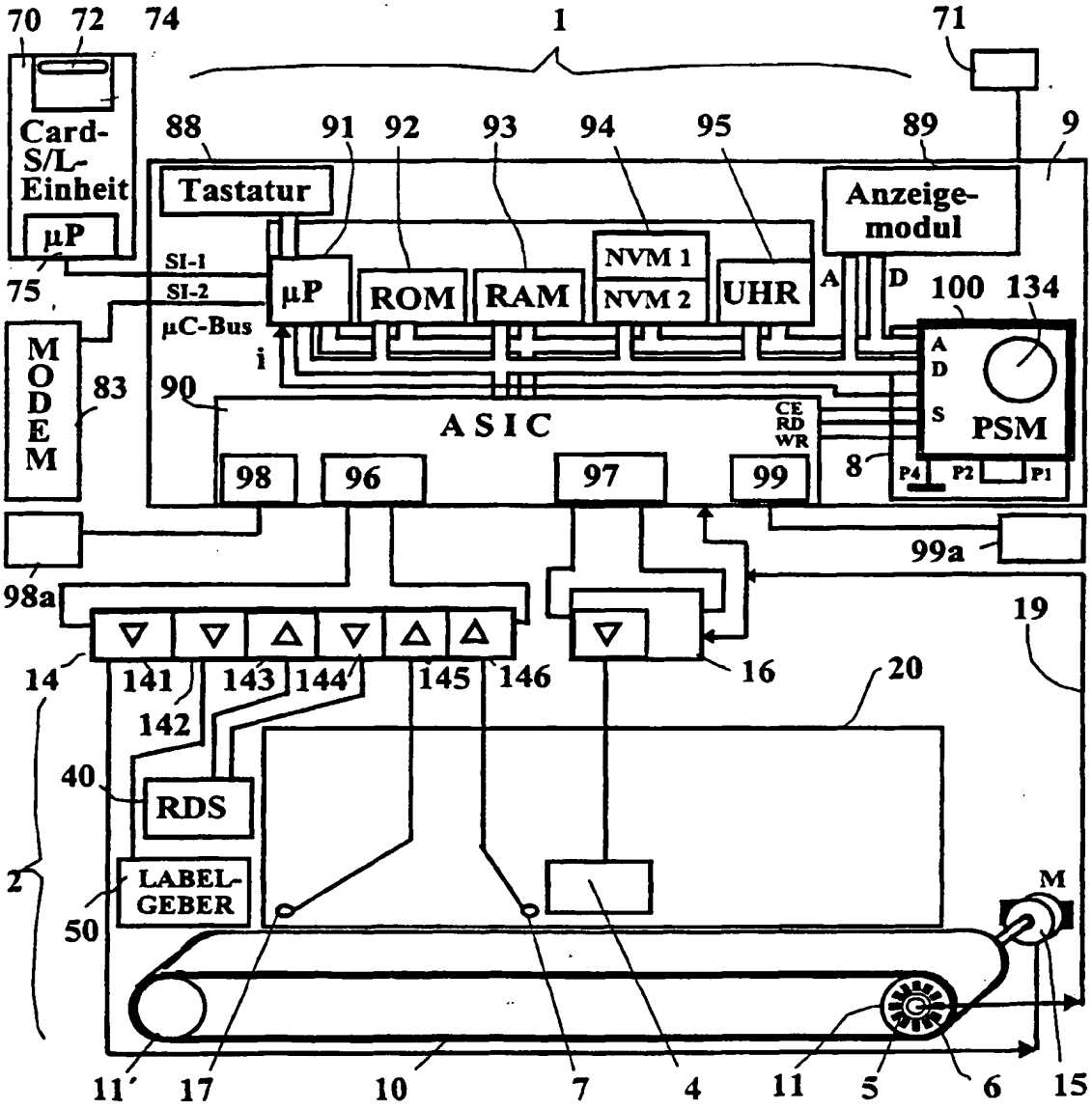
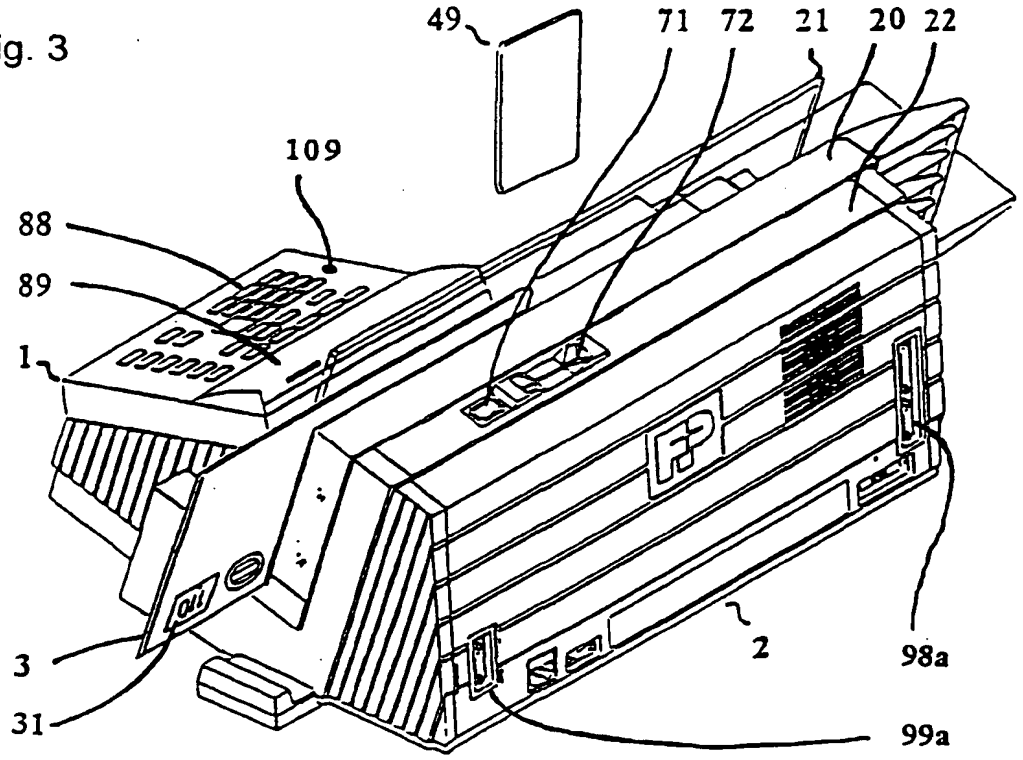

70
72
74
1
71
Card-
S/L-
Einheit
µP
75
88
91
92
93
94
95
89
9
Tastatur
Anzeige-
modul
SI-1
SI-2
µC-Bus
µP
ROM
RAM
NVM 1
NVM 2
UHR
A
D
100
134
MODEM
83
90
i
ASIC
CE
RD
WR
A
D
S
PSM
98
96
97
99
8
P4
P2
P1
99a
98a
19
14
141
142
143
144
145
146
16
20
40
RDS
2
LABEL-
GEBER
50
M
11'
17
10
7
4
11
5
6
15

Fig. 2

Fig. 3



Zustand Nr:	LEDs	leuchtet	blinkt	Aus	Anzeige	Bedeutung
220	R			X	Grün - leuchtend	OK
	G	X				
230	R	X			Rot - leuchtend	Fehler bei statischer Prüfung
	G			X		
240	R	X			Orange - leuchtend	Fehler bei dynamischer Prüfung
	G	X				
250	R		X		Rot - blinkend	lange Zeit kein Kontakt zur DZ
	G			X		
260	R			X	Grün - blinkend	Schlüssel ist nicht installiert
	G		X			
270	R		X		Orange - blinkend	suspekt
	G		X			
280	R	X			Rot leuchtend Orange blinkend	Temperatur zu hoch
	G		X			
290	R		X		Grün leuchtend Orange blinkend	Batteriewechsel erforderlich
	G	X				

Fig. 9

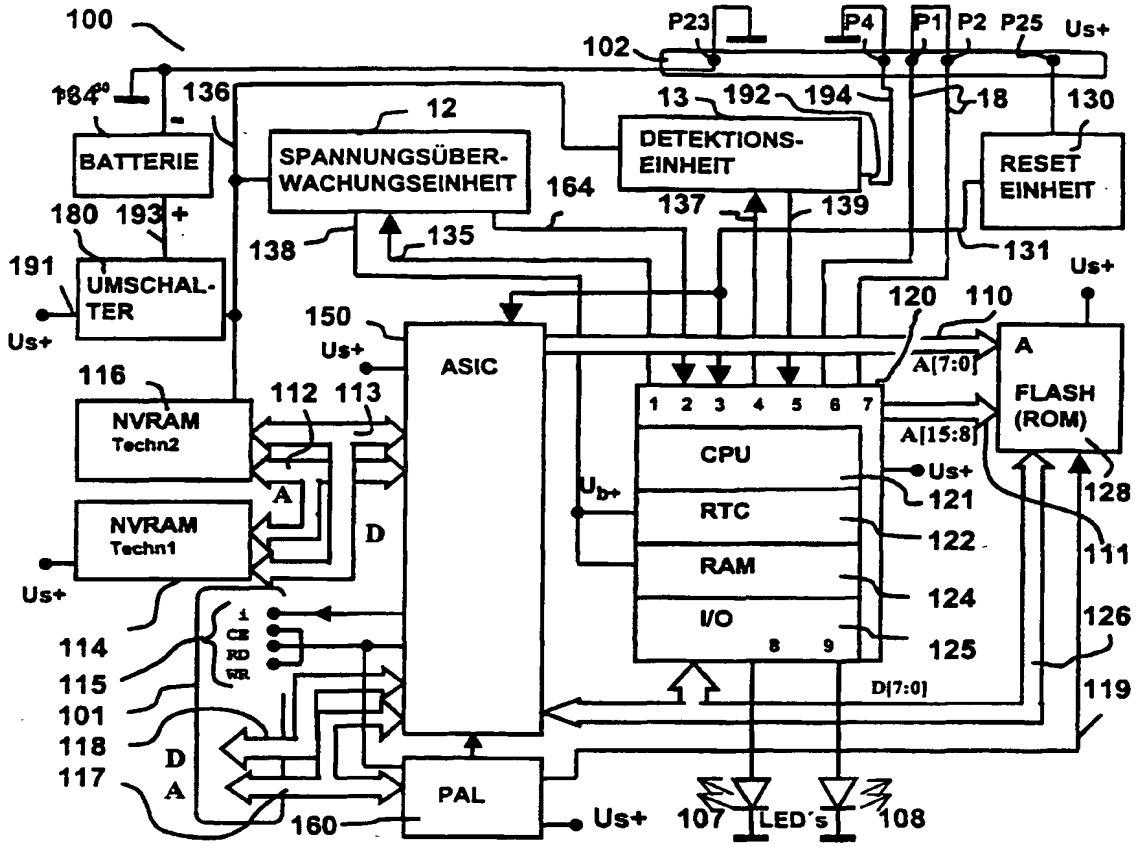

100
102
P23
P4
P1
P2
P25
Us+
184
136
12
13
192
194
18
130
BATTERIE
SPANNUNGSÜBER-
WACHUNGSEINHEIT
DETEKTIONS-
EINHEIT
RESET
EINHEIT
180
193
+
164
137
139
138
135
131
191
UMSCHAL-
TER
Us+
120
110
150
Us+
ASIC
A
A[7:0]
FLASH
(ROM)
116
112
113
1 2 3 4 5 6 7
A[15:8]
NVRAM
Techn2
CPU
Us+
121
128
A
U_{b+}
NVRAM
Techn1
RTC
122
D
RAM
111
Us+
124
I/O
126
114
CE
RD
WR
8 9
125
D[7:0]
115
119
101
118
D
117
A
PAL
160
Us+
107
LED's
108

Fig. 4

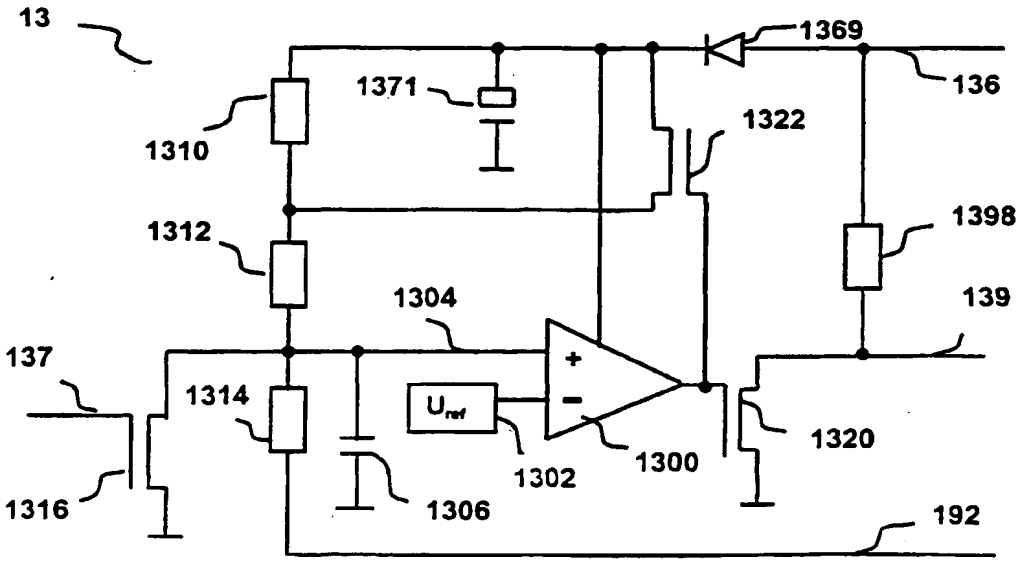

13
1369
1371
136
1310
1322
1312
1398
1304
139
137
+
1314
U_{ref}
1320
1302
1300
1316
1306
192

Fig. 5

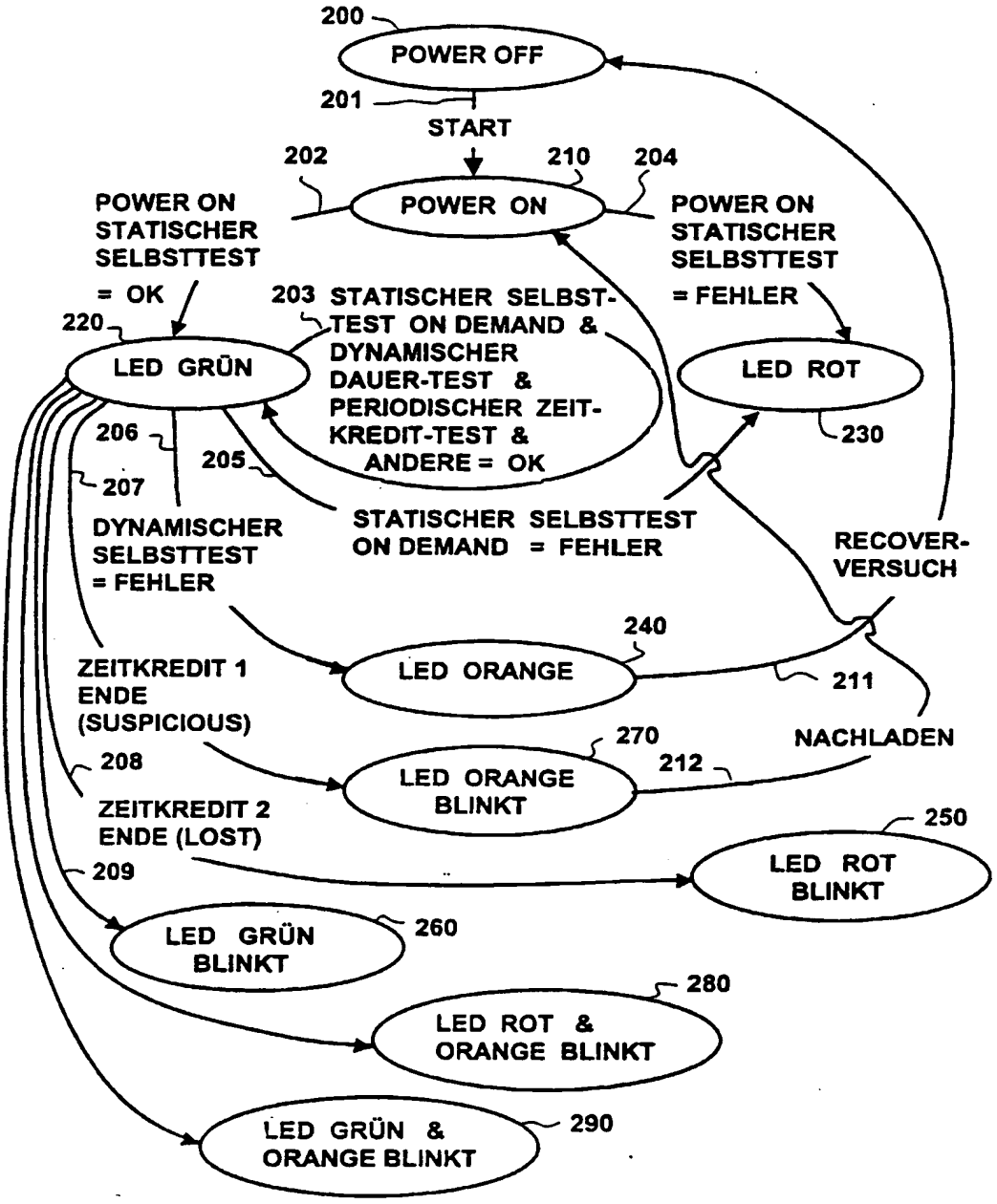

200
POWER OFF
201
START
202
210
204
POWER ON
POWER ON STATISCHER SELBSTTEST = OK
POWER ON STATISCHER SELBSTTEST = FEHLER
203 STATISCHER SELBST-TEST ON DEMAND & DYNAMISCHER DAUER-TEST & PERIODISCHER ZEIT-KREDIT-TEST & ANDERE = OK
220
LED GRÜN
LED ROT
230
206
205
207
DYNAMISCHER SELBSTTEST = FEHLER
STATISCHER SELBSTTEST ON DEMAND = FEHLER
RECOVER-VERSUCH
240
LED ORANGE
211
ZEITKREDIT 1 ENDE (SUSPICIOUS)
NACHLADEN
270
208
212
LED ORANGE BLINKT
ZEITKREDIT 2 ENDE (LOST)
250
209
LED ROT BLINKT
LED GRÜN BLINKT
260
280
LED ROT & ORANGE BLINKT
LED GRÜN & ORANGE BLINKT
290

Fig. 10

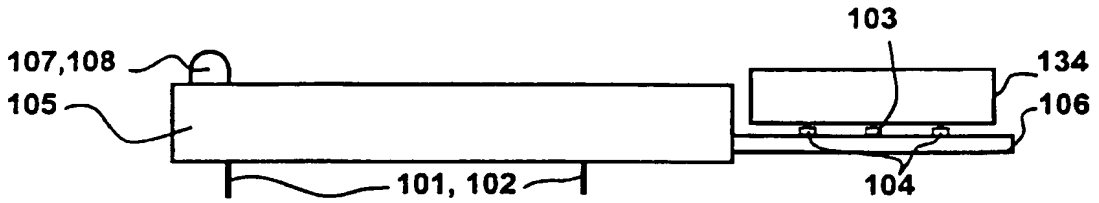


Fig. 6

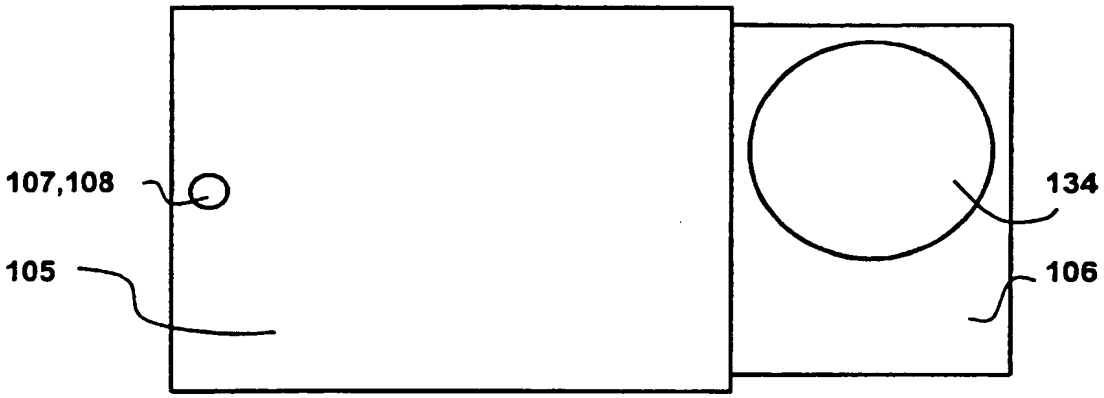


Fig. 7

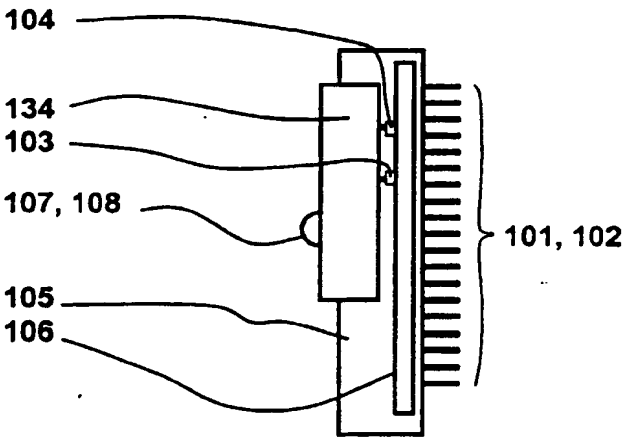


Fig. 8a

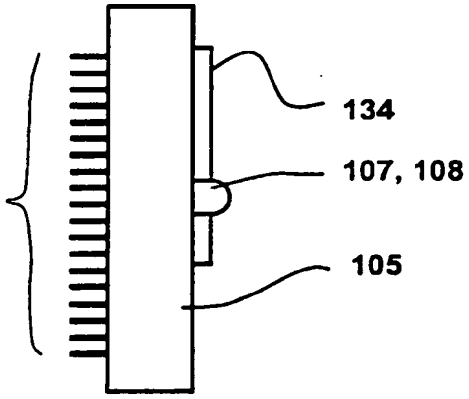


Fig. 8b

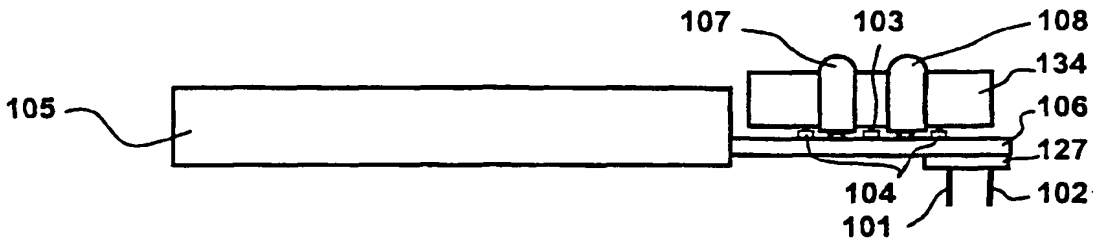


Fig. 11

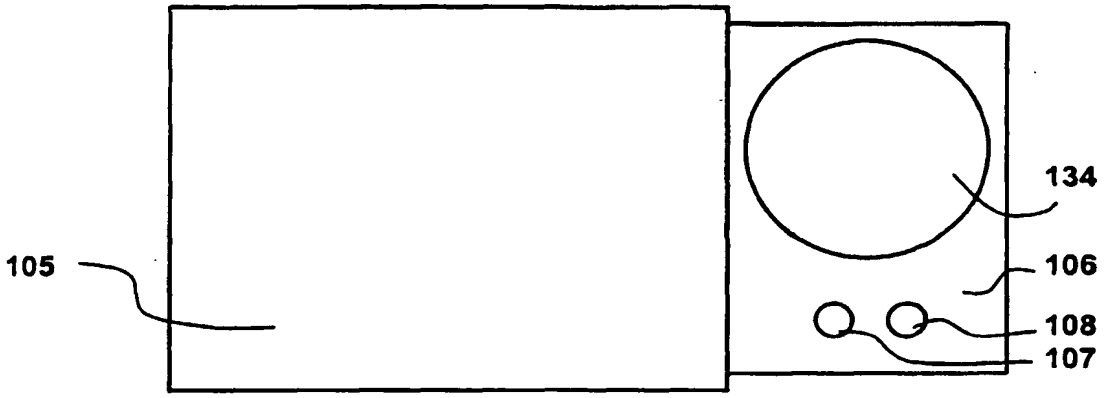


Fig. 12

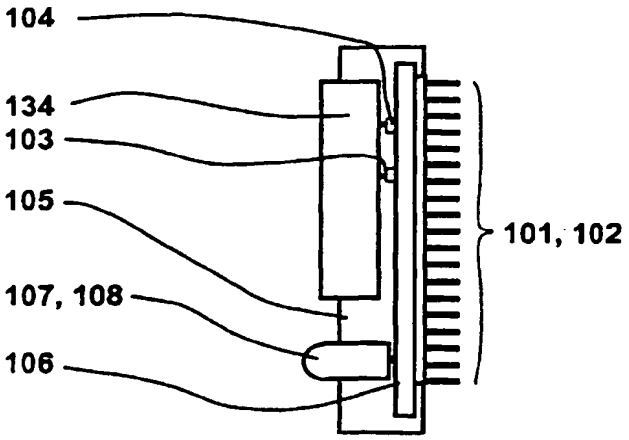


Fig. 13a

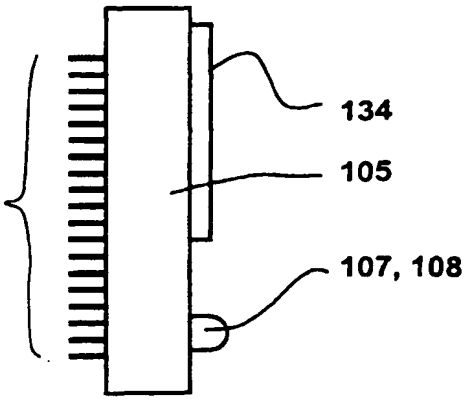


Fig. 13b